

深信服科技股份有限公司

综合评估报告

2023-05-31



**深信服科技股份有限公司**

**目录**

[1. 风险概述 3](#_Toc17698)

[1.1 资产概览 3](#_Toc30441)

[1.2 风险概况 3](#_Toc4593)

[2. 资产风险列表 4](#_Toc12203)

[3. 资产风险详情 4](#_Toc18998)

[4. 参考标准 6](#_Toc30162)

[4.1 单一系统漏洞风险等级评定标准 6](#_Toc27957)

[4.2 单一Web漏洞风险等级评定标准 6](#_Toc24925)

# 风险概述

本次评估共涉及7台主机，最终发现存在安全风险的主机有7台。

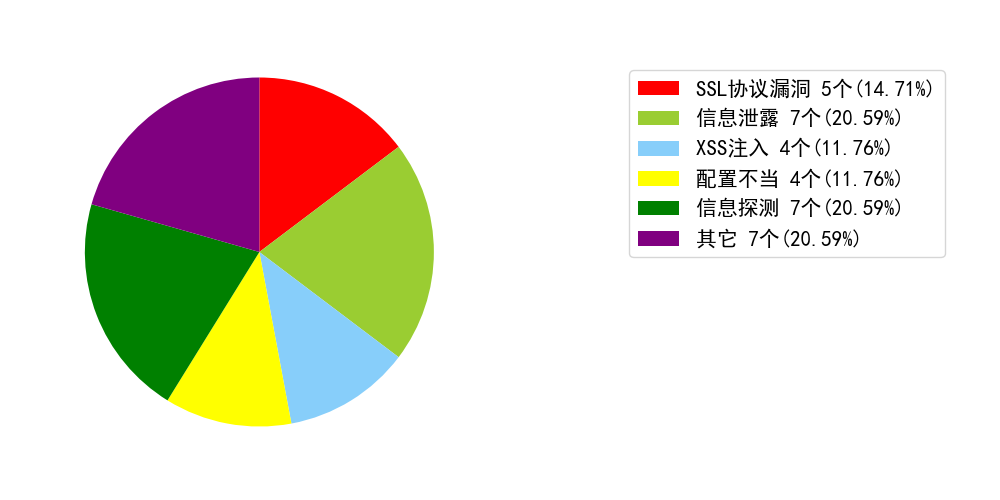
## 资产概览

本次评估服务，我们对您的信息资产进行了全面的评估扫描，发现风险的资产如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | IP地址/URL | 高 | 中 | 低 | 信息 | 总计 |
| 1 | 10.194.96.200 | 2 | 13 | 3 | 0 | 18 |
| 2 | 10.194.96.198 | 2 | 10 | 2 | 0 | 14 |
| 3 | 192.168.7.50 | 2 | 10 | 2 | 0 | 14 |
| 4 | 10.194.96.195 | 1 | 14 | 19 | 0 | 34 |
| 5 | 10.194.96.199 | 1 | 12 | 21 | 0 | 34 |
| 6 | 10.194.96.197 | 1 | 12 | 17 | 0 | 30 |
| 7 | 10.194.96.196 | 1 | 11 | 17 | 0 | 29 |

## 风险概况

本次评估服务，我们对您的信息资产进行了全面的漏洞扫描，漏洞分布如下：



发现关键风险如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **漏洞名称** | **风险等级** | **影响资产** | **资产数** |
| 1 | Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886) | 高 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 2 | Openssh 命令注入漏洞(CVE-2020-15778) | 高 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 3 | OpenSSH 安全漏洞(CVE-2021-28041) | 高 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 4 | 无效的自签名SSL证书 | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.19910.194.96.200 | 5 |
| 5 | 检测到目标服务支持SSL弱加密算法 | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.19910.194.96.200 | 5 |
| 6 | SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808) | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 7 | SSL/TLS协议信息泄露漏洞(CVE-2016-2183) | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 8 | Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794) | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 9 | 终端服务加密级别为中或低 | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 10 | 终端服务未使用网络级别身份验证（NLA） | 中 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 11 | OpenSSH 访问控制错误漏洞(CVE-2018-20685) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 12 | OpenSSH 访问控制错误漏洞 (CVE-2019-6109) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 13 | OpenSSH 访问控制错误漏洞 (CVE-2019-6110) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 14 | OpenSSH 输入验证错误漏洞 (CVE-2019-6111) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 15 | OpenSSH 信息泄漏漏洞 (CVE-2018-15919) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 16 | OpenSSH 安全漏洞(CVE-2017-15906) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 17 | OpenSSH 安全漏洞(CVE-2016-20012) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 18 | OpenSSH信息泄露漏洞（CVE-2020-14145） | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 19 | OpenSSH 安全漏洞(CVE-2021-41617) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 20 | OpenSSH 访问限制绕过漏洞(CVE-2018-20685) | 中 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 21 | SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞 (CVE-2015-4000) | 中 | 10.194.96.19710.194.96.199 | 2 |
| 22 | 服务器支持 SSL Insecure Renegotiation(CVE-2009-3555) | 中 | 10.194.96.19510.194.96.200 | 2 |
| 23 | WU-FTPD QUOTE PASV强制核心转储信息泄露(CVE-1999-0075) | 中 | 10.194.96.195 | 1 |
| 24 | ICMP时间戳请求远程日期泄露(CVE-1999-0524) | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.19810.194.96.19910.194.96.200192.168.7.50 | 7 |
| 25 | 检测到目标主机加密通信支持的SSL加密算法 | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.19910.194.96.200 | 5 |
| 26 | 未设置X-Content-Type-Options响应头 | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 27 | 未设置X-XSS-Protection响应头 | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 28 | 未设置Strict-Transport-Security响应头 | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 29 | X-Frame-Options头未设置 | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 30 | SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566) | 低 | 10.194.96.19510.194.96.19610.194.96.19710.194.96.199 | 4 |
| 31 | OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161) | 低 | 10.194.96.19810.194.96.200192.168.7.50 | 3 |
| 32 | 未加密的FTP协议 | 低 | 10.194.96.195 | 1 |

# 资产风险列表

存在风险的资产列表如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **主机IP/URL** | **漏洞列表** | **风险等级** |
| 1 | 10.194.96.197 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞 (CVE-2015-4000)SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】X-Frame-Options头未设置【原理扫描】无效的自签名SSL证书【原理扫描】未设置Strict-Transport-Security响应头【原理扫描】未设置X-Content-Type-Options响应头【原理扫描】未设置X-XSS-Protection响应头【原理扫描】检测到目标主机加密通信支持的SSL加密算法【原理扫描】检测到目标服务支持SSL弱加密算法【原理扫描】终端服务加密级别为中或低【原理扫描】终端服务未使用网络级别身份验证（NLA）【原理扫描】 | 高 |
| 2 | 10.194.96.198 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】OpenSSH 信息泄漏漏洞 (CVE-2018-15919)Openssh 命令注入漏洞(CVE-2020-15778)OpenSSH 安全漏洞(CVE-2016-20012)OpenSSH 安全漏洞(CVE-2017-15906)OpenSSH 安全漏洞(CVE-2021-28041)OpenSSH 安全漏洞(CVE-2021-41617)OpenSSH 访问控制错误漏洞 (CVE-2019-6109)OpenSSH 访问控制错误漏洞 (CVE-2019-6110)OpenSSH 访问控制错误漏洞(CVE-2018-20685)OpenSSH 访问限制绕过漏洞(CVE-2018-20685)OpenSSH 输入验证错误漏洞 (CVE-2019-6111)OpenSSH信息泄露漏洞（CVE-2020-14145） | 高 |
| 3 | 10.194.96.196 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】X-Frame-Options头未设置【原理扫描】无效的自签名SSL证书【原理扫描】未设置Strict-Transport-Security响应头【原理扫描】未设置X-Content-Type-Options响应头【原理扫描】未设置X-XSS-Protection响应头【原理扫描】检测到目标主机加密通信支持的SSL加密算法【原理扫描】检测到目标服务支持SSL弱加密算法【原理扫描】终端服务加密级别为中或低【原理扫描】终端服务未使用网络级别身份验证（NLA）【原理扫描】 | 高 |
| 4 | 10.194.96.195 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】WU-FTPD QUOTE PASV强制核心转储信息泄露(CVE-1999-0075)【原理扫描】X-Frame-Options头未设置【原理扫描】无效的自签名SSL证书【原理扫描】服务器支持 SSL Insecure Renegotiation(CVE-2009-3555)【原理扫描】未加密的FTP协议【原理扫描】未设置Strict-Transport-Security响应头【原理扫描】未设置X-Content-Type-Options响应头【原理扫描】未设置X-XSS-Protection响应头【原理扫描】检测到目标主机加密通信支持的SSL加密算法【原理扫描】检测到目标服务支持SSL弱加密算法【原理扫描】终端服务加密级别为中或低【原理扫描】终端服务未使用网络级别身份验证（NLA）【原理扫描】 | 高 |
| 5 | 10.194.96.199 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞 (CVE-2015-4000)SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】X-Frame-Options头未设置【原理扫描】无效的自签名SSL证书【原理扫描】未设置Strict-Transport-Security响应头【原理扫描】未设置X-Content-Type-Options响应头【原理扫描】未设置X-XSS-Protection响应头【原理扫描】检测到目标主机加密通信支持的SSL加密算法【原理扫描】检测到目标服务支持SSL弱加密算法【原理扫描】终端服务加密级别为中或低【原理扫描】终端服务未使用网络级别身份验证（NLA）【原理扫描】 | 高 |
| 6 | 10.194.96.200 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】OpenSSH 信息泄漏漏洞 (CVE-2018-15919)Openssh 命令注入漏洞(CVE-2020-15778)OpenSSH 安全漏洞(CVE-2016-20012)OpenSSH 安全漏洞(CVE-2017-15906)OpenSSH 安全漏洞(CVE-2021-28041)OpenSSH 安全漏洞(CVE-2021-41617)OpenSSH 访问控制错误漏洞 (CVE-2019-6109)OpenSSH 访问控制错误漏洞 (CVE-2019-6110)OpenSSH 访问控制错误漏洞(CVE-2018-20685)OpenSSH 访问限制绕过漏洞(CVE-2018-20685)OpenSSH 输入验证错误漏洞 (CVE-2019-6111)OpenSSH信息泄露漏洞（CVE-2020-14145）无效的自签名SSL证书【原理扫描】服务器支持 SSL Insecure Renegotiation(CVE-2009-3555)【原理扫描】检测到目标主机加密通信支持的SSL加密算法【原理扫描】检测到目标服务支持SSL弱加密算法【原理扫描】 | 高 |
| 7 | 192.168.7.50 | ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】OpenSSH 信息泄漏漏洞 (CVE-2018-15919)Openssh 命令注入漏洞(CVE-2020-15778)OpenSSH 安全漏洞(CVE-2016-20012)OpenSSH 安全漏洞(CVE-2017-15906)OpenSSH 安全漏洞(CVE-2021-28041)OpenSSH 安全漏洞(CVE-2021-41617)OpenSSH 访问控制错误漏洞 (CVE-2019-6109)OpenSSH 访问控制错误漏洞 (CVE-2019-6110)OpenSSH 访问控制错误漏洞(CVE-2018-20685)OpenSSH 访问限制绕过漏洞(CVE-2018-20685)OpenSSH 输入验证错误漏洞 (CVE-2019-6111)OpenSSH信息泄露漏洞（CVE-2020-14145） | 高 |

# 资产风险详情

## 10.194.96.197

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-2021-00130 | |
| 端口(服务)： | 3389 | |
| 风险描述： | Windows是一款由美国微软公司开发的窗口化操作系统。凭据安全支持提供程序协议 (CredSSP) 中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在目标系统上中继用户凭据并使用其执行代码。 | |
| 危害影响： | 攻击者可以利用此漏洞执行任意代码 | |
| 解决方案： | Microsoft 已经为此发布了一个安全公告（CVE-2018-0886）以及相应补丁:CVE-2018-0886: Microsoft Windows CredSSP 远程执行代码漏洞.链接https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 参考资料： | https://msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-0886 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201803-438 | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 3389 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞 (CVE-2015-4000)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2019-50051 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出Web浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL在传输层对网络连接进行加密。传输层安全TLS（Transport Layer Security），IETF对SSL协议标准化（RFC 2246）后的产物，与SSL 3.0差异很小。当服务器SSL/TLS的瞬时Diffie-Hellman公共密钥小于等于1024位时，存在可以恢复纯文本信息的风险。DHE man-in-the-middle protection (Logjam)--------------------------------------------------------https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/https://en.wikipedia.org/wiki/DiffieE28093Hellman\_key\_exchange#Security | |
| 危害影响： | 导致信息泄露 | |
| 解决方案： | 一. http服务器相关配置1.首先生成大于1024bit(例如2048bit)的dhkeyopenssl dhparam -out dhparams.pem 20482.然后在对应服务器中配置Apache2.4.8及以后版本使用如下配置命令配置（http.conf中或者对应的虚拟主机配置文件中添加）SSLOpenSSLConfCmd DHParameters &#34;{path to dhparams.pem}&#34; Apache2.4.7版本Apache2.2.31版本及以后版本redhat debian等大多发行版中最新Apache2.2.x通过把dhparams.pem的内容直接附加到证书文件后 Apache2.4.7之前2.4.x版本Apache2.2.31之前版本dhparam默认为1024bit 无法修改nginx使用如下命令配置（在对应的虚拟主机配置文件nginx.conf中server字段内添加）ssl\_dhparam {path to dhparams.pem}二.如果服务器配置无法修改，例如Apache2.2.31之前版本，可以禁用DHE系列算法，采用保密性更好的ECDHE系列算法，如果ECDHE不可用可以采用普通的 RSA。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-4000 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2015-03367 | |
| CNNVD编号： | CNNVD-201505-428 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 3389 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00055 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程桌面协议服务器（终端服务）的远程版本容易受到中间人（MiTM）攻击。 RDP客户端在设置加密时不会尝试验证服务器的身份。 能够拦截来自RDP服务器的流量的攻击者可以在不检测到的情况下与客户端和服务器建立加密。 这种性质的MiTM攻击将允许攻击者获取传输的任何敏感信息，包括身份验证凭据。这个缺陷的存在是因为RDP服务器在mstlsapi.dll库中存储了一个硬编码的RSA私钥。 任何有权访问此文件的本地用户（在任何Windows系统上）都可以检索密钥并将其用于此攻击。 | |
| 危害影响： | 允许攻击者获取传输的任何敏感信息，包括身份验证凭据。 | |
| 解决方案： | - 如果支持，则强制使用SSL作为此服务的传输层，或/和, - 选择“仅允许来自运行具有网络级别身份验证的远程桌面的计算机的连接”设置（如果可用）。 | |
| 参考资料： | https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Configuring-Terminal-Servers-for-Server-Authentication-to/ba-p/246602http://technet.microsoft.com/en-us/library/cc782610.aspxhttp://www.oxid.it/downloads/rdp-gbu.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2005-1794 | |
| BID编号： | 13818 | |
| CNVD编号： | CNVD-2009-07766 | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **终端服务未使用网络级别身份验证（NLA）【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00078 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务未配置为仅使用网络级别身份验证（NLA）。 NLA使用凭据安全支持提供程序（CredSSP）协议通过TLS / SSL或Kerberos机制执行强大的服务器身份验证，从而防止中间人攻击。除了改善身份验证外，NLA还可以通过在建立完整的RDP连接之前完成用户身份验证来帮助保护远程计算机免受恶意用户和软件的侵害。 | |
| 危害影响： | 未使用该认证的远程主机受攻击的风险等级高。 | |
| 解决方案： | 在远程RDP服务器上启用网络级别身份验证（NLA）。通常，这是在Windows上“系统”设置的“远程”选项卡上完成的。 | |
| 参考资料： | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 5986 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **终端服务加密级别为中或低【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00077 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务服务未配置为使用强加密。将此服务与弱加密一起使用，可能使攻击者更容易窃听通信并获取屏幕截图。 | |
| 危害影响： | 该配置的远程主机受到攻击的风险等级高。 | |
| 解决方案： | 将RDP加密级别更改为以下一项：3.高4.符合FIPS | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 5986 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.197 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.197 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.197:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

## 10.194.96.198

|  |  |  |
| --- | --- | --- |
| **Openssh 命令注入漏洞(CVE-2020-15778)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-02635 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 8.3p1及之前版本中的scp的scp.c文件存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。 | |
| 危害影响： | 影响OpenSSH:8.4p1以下版本(含) | |
| 解决方案： | 可以禁用scp，改用rsync等缓解风险（可能会导致小文件机器内拷贝变慢） | |
| 参考资料： | https://www.openssh.com/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-15778 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202007-1519 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-28041)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-06510 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。 | |
| 危害影响： | 影响OpenSSH:8.5以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2021-28041http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-202103-527 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-28041 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202103-527 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2017-15906)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-06522 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.6之前的版本中的sftp-server.c文件的‘process\_open’函数存在安全漏洞，该漏洞源于程序在只读模式下没有正确的阻止写入操作。攻击者可利用该漏洞创建长度为零的文件。 | |
| 危害影响： | 影响OpenSSH:7.6以下版本 | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/txt/release-7.6 | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2017-15906http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201710-1230 | |
| 协议类型： | - | |
| CVE编号： | CVE-2017-15906 | |
| BID编号： | 101552 | |
| CNVD编号： | CNVD-2017-36017 | |
| CNNVD编号： | CNNVD-201710-1230 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 输入验证错误漏洞 (CVE-2019-6111)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00644 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中的scp client实用程序存在安全漏洞，该漏洞源于程序错误的验证了对象名称。攻击者可利用该漏洞覆盖文件。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-767https://bugzilla.redhat.com/show\_bug.cgi?id=1677794https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6111 | |
| BID编号： | 106741 | |
| CNVD编号： | CNVD-2019-02499 | |
| CNNVD编号： | CNNVD-201901-767 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0004-50004 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本中的scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名利用该漏洞造成SSH服务器绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/。 | |
| 参考资料： | http://www.securityfocus.com/bid/106531 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： | 106531 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问限制绕过漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-13834 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一套用于安全访问远程计算机的连接工具。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本，scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名，利用该漏洞绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:8.0版本以下版本 | |
| 解决方案： | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20685 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH信息泄露漏洞（CVE-2020-14145）** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10927 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。OpenSSH 5.7至8.3版本的客户端存在信息泄露漏洞。该漏洞产生的原因是OpenSSH客户端中的可观察到的差异会导致算法协商过程中的信息泄露。中间人攻击者可利用该漏洞攻击初始连接尝试。 | |
| 危害影响： | 影响OpenSSH:5.7版本(含)到8.4版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.openbsd.org/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145 | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-14145 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202006-1822 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-41617)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10928 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 6.2到8.8之前版本存在安全漏洞。该漏洞源于允许权限提升，因为补充组未按预期初始化。 | |
| 危害影响： | 影响OpenSSH:6.2版本(含)到8.8版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41617 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-41617 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1695 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6109)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00642 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中存在安全漏洞，该漏洞源于程序没有对字符进行编码。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-467https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://usn.ubuntu.com/3885-1/https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6109 | |
| BID编号： | 106843 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-467 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2016-20012)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10926 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 8.7之前版本存在安全漏洞，允许远程攻击者怀疑 SSH 服务器知道用户名和公钥的特定组合，以测试这种怀疑是否正确。 发生这种情况是因为仅当该组合对登录会话有效时才会发送质询。 | |
| 危害影响： | 影响OpenSSH:8.7版本(含)以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/pull/270 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20012 | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-20012 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1073 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 信息泄漏漏洞 (CVE-2018-15919)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00645 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.8及之前版本中的auth-gss2.c文件存在信息泄漏漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。\*重点:使用GSS2时会存在漏洞 | |
| 危害影响： | 影响OpenSSH:5.9版本(含)到7.8版本(含) | |
| 解决方案： | 建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201808-902http://www.securityfocus.com/bid/105163http://seclists.org/oss-sec/2018/q3/180https://security.netapp.com/advisory/ntap-20181221-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-15919 | |
| BID编号： | 105163 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201808-902 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6110)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00643 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。SCP（Secure Copy Protocol）是一个远程文件复制协议。OpenSSH中的SCP客户端实用程序存在安全漏洞。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-468https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://security.netapp.com/advisory/ntap-20190213-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6110 | |
| BID编号： | 106836 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-468 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2021-00587 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。 | |
| 危害影响： | 攻击者可以利用该信息进行下一步攻击。 | |
| 解决方案： | 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2008-5161 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2009-12630 | |
| CNNVD编号： | CNNVD-200811-32 | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 22 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

## 10.194.96.196

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-2021-00130 | |
| 端口(服务)： | 3389 | |
| 风险描述： | Windows是一款由美国微软公司开发的窗口化操作系统。凭据安全支持提供程序协议 (CredSSP) 中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在目标系统上中继用户凭据并使用其执行代码。 | |
| 危害影响： | 攻击者可以利用此漏洞执行任意代码 | |
| 解决方案： | Microsoft 已经为此发布了一个安全公告（CVE-2018-0886）以及相应补丁:CVE-2018-0886: Microsoft Windows CredSSP 远程执行代码漏洞.链接https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 参考资料： | https://msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-0886 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201803-438 | |

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00055 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程桌面协议服务器（终端服务）的远程版本容易受到中间人（MiTM）攻击。 RDP客户端在设置加密时不会尝试验证服务器的身份。 能够拦截来自RDP服务器的流量的攻击者可以在不检测到的情况下与客户端和服务器建立加密。 这种性质的MiTM攻击将允许攻击者获取传输的任何敏感信息，包括身份验证凭据。这个缺陷的存在是因为RDP服务器在mstlsapi.dll库中存储了一个硬编码的RSA私钥。 任何有权访问此文件的本地用户（在任何Windows系统上）都可以检索密钥并将其用于此攻击。 | |
| 危害影响： | 允许攻击者获取传输的任何敏感信息，包括身份验证凭据。 | |
| 解决方案： | - 如果支持，则强制使用SSL作为此服务的传输层，或/和, - 选择“仅允许来自运行具有网络级别身份验证的远程桌面的计算机的连接”设置（如果可用）。 | |
| 参考资料： | https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Configuring-Terminal-Servers-for-Server-Authentication-to/ba-p/246602http://technet.microsoft.com/en-us/library/cc782610.aspxhttp://www.oxid.it/downloads/rdp-gbu.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2005-1794 | |
| BID编号： | 13818 | |
| CNVD编号： | CNVD-2009-07766 | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 3389 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **终端服务未使用网络级别身份验证（NLA）【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00078 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务未配置为仅使用网络级别身份验证（NLA）。 NLA使用凭据安全支持提供程序（CredSSP）协议通过TLS / SSL或Kerberos机制执行强大的服务器身份验证，从而防止中间人攻击。除了改善身份验证外，NLA还可以通过在建立完整的RDP连接之前完成用户身份验证来帮助保护远程计算机免受恶意用户和软件的侵害。 | |
| 危害影响： | 未使用该认证的远程主机受攻击的风险等级高。 | |
| 解决方案： | 在远程RDP服务器上启用网络级别身份验证（NLA）。通常，这是在Windows上“系统”设置的“远程”选项卡上完成的。 | |
| 参考资料： | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 5986 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 5986 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **终端服务加密级别为中或低【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00077 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务服务未配置为使用强加密。将此服务与弱加密一起使用，可能使攻击者更容易窃听通信并获取屏幕截图。 | |
| 危害影响： | 该配置的远程主机受到攻击的风险等级高。 | |
| 解决方案： | 将RDP加密级别更改为以下一项：3.高4.符合FIPS | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 3389 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.196 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.196 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.196:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

## 10.194.96.195

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-2021-00130 | |
| 端口(服务)： | 3389 | |
| 风险描述： | Windows是一款由美国微软公司开发的窗口化操作系统。凭据安全支持提供程序协议 (CredSSP) 中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在目标系统上中继用户凭据并使用其执行代码。 | |
| 危害影响： | 攻击者可以利用此漏洞执行任意代码 | |
| 解决方案： | Microsoft 已经为此发布了一个安全公告（CVE-2018-0886）以及相应补丁:CVE-2018-0886: Microsoft Windows CredSSP 远程执行代码漏洞.链接https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 参考资料： | https://msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-0886 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201803-438 | |

|  |  |  |
| --- | --- | --- |
| **终端服务未使用网络级别身份验证（NLA）【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00078 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务未配置为仅使用网络级别身份验证（NLA）。 NLA使用凭据安全支持提供程序（CredSSP）协议通过TLS / SSL或Kerberos机制执行强大的服务器身份验证，从而防止中间人攻击。除了改善身份验证外，NLA还可以通过在建立完整的RDP连接之前完成用户身份验证来帮助保护远程计算机免受恶意用户和软件的侵害。 | |
| 危害影响： | 未使用该认证的远程主机受攻击的风险等级高。 | |
| 解决方案： | 在远程RDP服务器上启用网络级别身份验证（NLA）。通常，这是在Windows上“系统”设置的“远程”选项卡上完成的。 | |
| 参考资料： | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 3389 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **终端服务加密级别为中或低【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00077 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务服务未配置为使用强加密。将此服务与弱加密一起使用，可能使攻击者更容易窃听通信并获取屏幕截图。 | |
| 危害影响： | 该配置的远程主机受到攻击的风险等级高。 | |
| 解决方案： | 将RDP加密级别更改为以下一项：3.高4.符合FIPS | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 5986 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 5986 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **服务器支持 SSL Insecure Renegotiation(CVE-2009-3555)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2021-00952 | |
| 端口(服务)： | 9000 | |
| 风险描述： | 服务器支持SSL Insecure Renegotiation该漏洞是由于SSL协议设计考虑不周导致的，利用这个漏洞能够在受保护的TLS/SSL连接上引入信息，从而发送流量来欺骗经验证的客户端，造成中间人攻击。 | |
| 危害影响： | 远程攻击者可以利用此漏洞执进行中间人攻击 | |
| 解决方案： | 建议升级openssl来进行修复，openssl-0.98m之后的版本就已经修复了该漏洞，使用了Secure Renegotiation。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2009-3555 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2011-1530 | |
| CNNVD编号： | CNNVD-200911-069 | |

|  |  |  |
| --- | --- | --- |
| **WU-FTPD QUOTE PASV强制核心转储信息泄露(CVE-1999-0075)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2021-00889 | |
| 端口(服务)： | 8021 | |
| 风险描述： | 远程FTP服务器无法处理登录用户的QUOTE PASV请求。攻击者可以发送特制请求以使服务死亡并转储核心。核心文件包含所有用户的用户名和密码。 | |
| 危害影响： | 攻击者可以发送特制请求以使服务死亡并转储核心。, , 核心文件包含所有用户的用户名和密码。 | |
| 解决方案： | 将FTP服务器升级到最新版本。 | |
| 参考资料： | https://docs.freebsd.org/cgi/getmsg.cgi?fetch=113849+0+archive/1996/freebsd-bugs/19961013.freebsd-bugshttp://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199610-006 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0075 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199610-006 | |

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00055 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程桌面协议服务器（终端服务）的远程版本容易受到中间人（MiTM）攻击。 RDP客户端在设置加密时不会尝试验证服务器的身份。 能够拦截来自RDP服务器的流量的攻击者可以在不检测到的情况下与客户端和服务器建立加密。 这种性质的MiTM攻击将允许攻击者获取传输的任何敏感信息，包括身份验证凭据。这个缺陷的存在是因为RDP服务器在mstlsapi.dll库中存储了一个硬编码的RSA私钥。 任何有权访问此文件的本地用户（在任何Windows系统上）都可以检索密钥并将其用于此攻击。 | |
| 危害影响： | 允许攻击者获取传输的任何敏感信息，包括身份验证凭据。 | |
| 解决方案： | - 如果支持，则强制使用SSL作为此服务的传输层，或/和, - 选择“仅允许来自运行具有网络级别身份验证的远程桌面的计算机的连接”设置（如果可用）。 | |
| 参考资料： | https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Configuring-Terminal-Servers-for-Server-Authentication-to/ba-p/246602http://technet.microsoft.com/en-us/library/cc782610.aspxhttp://www.oxid.it/downloads/rdp-gbu.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2005-1794 | |
| BID编号： | 13818 | |
| CNVD编号： | CNVD-2009-07766 | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 3389 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 9000 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 9000 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **未加密的FTP协议【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2021-00430 | |
| 端口(服务)： | 8021 | |
| 风险描述： | 远程主机的FTP服务允许使用未加密FTP | |
| 危害影响： | 远程攻击者可以利用此漏洞访问敏感信息 | |
| 解决方案： | 通过AUTH TLS开启FTPS | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.195 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.195 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.195:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

## 10.194.96.199

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-2021-00130 | |
| 端口(服务)： | 3389 | |
| 风险描述： | Windows是一款由美国微软公司开发的窗口化操作系统。凭据安全支持提供程序协议 (CredSSP) 中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在目标系统上中继用户凭据并使用其执行代码。 | |
| 危害影响： | 攻击者可以利用此漏洞执行任意代码 | |
| 解决方案： | Microsoft 已经为此发布了一个安全公告（CVE-2018-0886）以及相应补丁:CVE-2018-0886: Microsoft Windows CredSSP 远程执行代码漏洞.链接https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 参考资料： | https://msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2018-0886 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-0886 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201803-438 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 5986 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **终端服务未使用网络级别身份验证（NLA）【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00078 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务未配置为仅使用网络级别身份验证（NLA）。 NLA使用凭据安全支持提供程序（CredSSP）协议通过TLS / SSL或Kerberos机制执行强大的服务器身份验证，从而防止中间人攻击。除了改善身份验证外，NLA还可以通过在建立完整的RDP连接之前完成用户身份验证来帮助保护远程计算机免受恶意用户和软件的侵害。 | |
| 危害影响： | 未使用该认证的远程主机受攻击的风险等级高。 | |
| 解决方案： | 在远程RDP服务器上启用网络级别身份验证（NLA）。通常，这是在Windows上“系统”设置的“远程”选项卡上完成的。 | |
| 参考资料： | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 3389 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **Microsoft Windows远程桌面协议服务程序密钥泄露漏洞(CVE-2005-1794)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00055 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程桌面协议服务器（终端服务）的远程版本容易受到中间人（MiTM）攻击。 RDP客户端在设置加密时不会尝试验证服务器的身份。 能够拦截来自RDP服务器的流量的攻击者可以在不检测到的情况下与客户端和服务器建立加密。 这种性质的MiTM攻击将允许攻击者获取传输的任何敏感信息，包括身份验证凭据。这个缺陷的存在是因为RDP服务器在mstlsapi.dll库中存储了一个硬编码的RSA私钥。 任何有权访问此文件的本地用户（在任何Windows系统上）都可以检索密钥并将其用于此攻击。 | |
| 危害影响： | 允许攻击者获取传输的任何敏感信息，包括身份验证凭据。 | |
| 解决方案： | - 如果支持，则强制使用SSL作为此服务的传输层，或/和, - 选择“仅允许来自运行具有网络级别身份验证的远程桌面的计算机的连接”设置（如果可用）。 | |
| 参考资料： | https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Configuring-Terminal-Servers-for-Server-Authentication-to/ba-p/246602http://technet.microsoft.com/en-us/library/cc782610.aspxhttp://www.oxid.it/downloads/rdp-gbu.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2005-1794 | |
| BID编号： | 13818 | |
| CNVD编号： | CNVD-2009-07766 | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **终端服务加密级别为中或低【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00077 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程终端服务服务未配置为使用强加密。将此服务与弱加密一起使用，可能使攻击者更容易窃听通信并获取屏幕截图。 | |
| 危害影响： | 该配置的远程主机受到攻击的风险等级高。 | |
| 解决方案： | 将RDP加密级别更改为以下一项：3.高4.符合FIPS | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00045 | |
| 端口(服务)： | 3389 | |
| 风险描述： | RC4是美国软件开发者罗纳德-李维斯特（Ron Rivest）所研发的一套密钥长度可变的流加密算法。该算法由伪随机数生成器和异或运算组成，且支持加解密使用相同的密钥。TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。 | |
| 危害影响： | 影响SSL/TLS所有支持RC4加密算法的版本。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-2808 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201503-654 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00047 | |
| 端口(服务)： | 5986 | |
| 风险描述： | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 1、请在下列网页下载最新版本:https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016 | |
| 参考资料： | https://www.openssl.org/source/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-2183 | |
| BID编号： | 92630 | |
| CNVD编号： | CNVD-2016-06765 | |
| CNNVD编号： | CNNVD-201608-448 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞 (CVE-2015-4000)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2019-50051 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出Web浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL在传输层对网络连接进行加密。传输层安全TLS（Transport Layer Security），IETF对SSL协议标准化（RFC 2246）后的产物，与SSL 3.0差异很小。当服务器SSL/TLS的瞬时Diffie-Hellman公共密钥小于等于1024位时，存在可以恢复纯文本信息的风险。DHE man-in-the-middle protection (Logjam)--------------------------------------------------------https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/https://en.wikipedia.org/wiki/DiffieE28093Hellman\_key\_exchange#Security | |
| 危害影响： | 导致信息泄露 | |
| 解决方案： | 一. http服务器相关配置1.首先生成大于1024bit(例如2048bit)的dhkeyopenssl dhparam -out dhparams.pem 20482.然后在对应服务器中配置Apache2.4.8及以后版本使用如下配置命令配置（http.conf中或者对应的虚拟主机配置文件中添加）SSLOpenSSLConfCmd DHParameters &#34;{path to dhparams.pem}&#34; Apache2.4.7版本Apache2.2.31版本及以后版本redhat debian等大多发行版中最新Apache2.2.x通过把dhparams.pem的内容直接附加到证书文件后 Apache2.4.7之前2.4.x版本Apache2.2.31之前版本dhparam默认为1024bit 无法修改nginx使用如下命令配置（在对应的虚拟主机配置文件nginx.conf中server字段内添加）ssl\_dhparam {path to dhparams.pem}二.如果服务器配置无法修改，例如Apache2.2.31之前版本，可以禁用DHE系列算法，采用保密性更好的ECDHE系列算法，如果ECDHE不可用可以采用普通的 RSA。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2015-4000 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2015-03367 | |
| CNNVD编号： | CNNVD-201505-428 | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 5986 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00044 | |
| 端口(服务)： | 3389 | |
| 风险描述： | 远程主机支持在一个或多个密码组中使用 RC4。RC4 密码在伪随机字节流的生成中存在缺陷，导致引入了各种各样的小偏差，降低了其随机性。如果反复加密明文（例如 HTTP cookie），并且攻击者能够获得许多（即上千万）密文，则该攻击者可能会推测出明文。 | |
| 危害影响： | 攻击者可利用大量的密文推测明文，导致远程主机信息泄露。 | |
| 解决方案： | 如果可能，请重新配置受影响的应用程序以避免使用 RC4 密码。可以考虑在浏览器和 Web 服务器的支持下将 TLS 1.2 用于 AES-GCM 组。 | |
| 参考资料： | http://cr.yp.to/talks/2013.03.12/slides.pdfhttp://www.isg.rhul.ac.uk/tls/https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | |
| 协议类型： | - | |
| CVE编号： | CVE-2013-2566 | |
| BID编号： | 73684, 58796 | |
| CNVD编号： | CNVD-2015-02171,CNVD-2013-02724 | |
| CNNVD编号： | CNNVD-201503-654,CNNVD-201303-335 | |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:80User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:80User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:80User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:80User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置Strict-Transport-Security响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:47001User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-XSS-Protection响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | http://msdn.microsoft.com/en-us/library/dd565647%28v=vs.85%29.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **X-Frame-Options头未设置【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 危害影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： |  | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5986User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

|  |  |  |
| --- | --- | --- |
| **未设置X-Content-Type-Options响应头【原理扫描】** | | |
| 风险页面： | 10.194.96.199 | |
| 风险等级： | 低 | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |
| 风险举证： | 10.194.96.199 | |
| 请求： | GET / HTTP/1.1Host: 10.194.96.199:5985User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive\r\n\r\n |

## 10.194.96.200

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-28041)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-06510 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。 | |
| 危害影响： | 影响OpenSSH:8.5以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2021-28041http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-202103-527 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-28041 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202103-527 | |

|  |  |  |
| --- | --- | --- |
| **Openssh 命令注入漏洞(CVE-2020-15778)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-02635 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 8.3p1及之前版本中的scp的scp.c文件存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。 | |
| 危害影响： | 影响OpenSSH:8.4p1以下版本(含) | |
| 解决方案： | 可以禁用scp，改用rsync等缓解风险（可能会导致小文件机器内拷贝变慢） | |
| 参考资料： | https://www.openssh.com/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-15778 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202007-1519 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2016-20012)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10926 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 8.7之前版本存在安全漏洞，允许远程攻击者怀疑 SSH 服务器知道用户名和公钥的特定组合，以测试这种怀疑是否正确。 发生这种情况是因为仅当该组合对登录会话有效时才会发送质询。 | |
| 危害影响： | 影响OpenSSH:8.7版本(含)以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/pull/270 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20012 | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-20012 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1073 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0004-50004 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本中的scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名利用该漏洞造成SSH服务器绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/。 | |
| 参考资料： | http://www.securityfocus.com/bid/106531 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： | 106531 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标服务支持SSL弱加密算法【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00048 | |
| 端口(服务)： | 800 | |
| 风险描述： | 远程主机使用的SSL加密支持弱加密算法或根本就不加密。 | |
| 危害影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 禁用已知弱加密算法 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2017-15906)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-06522 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.6之前的版本中的sftp-server.c文件的‘process\_open’函数存在安全漏洞，该漏洞源于程序在只读模式下没有正确的阻止写入操作。攻击者可利用该漏洞创建长度为零的文件。 | |
| 危害影响： | 影响OpenSSH:7.6以下版本 | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/txt/release-7.6 | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2017-15906http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201710-1230 | |
| 协议类型： | - | |
| CVE编号： | CVE-2017-15906 | |
| BID编号： | 101552 | |
| CNVD编号： | CNVD-2017-36017 | |
| CNNVD编号： | CNNVD-201710-1230 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH信息泄露漏洞（CVE-2020-14145）** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10927 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。OpenSSH 5.7至8.3版本的客户端存在信息泄露漏洞。该漏洞产生的原因是OpenSSH客户端中的可观察到的差异会导致算法协商过程中的信息泄露。中间人攻击者可利用该漏洞攻击初始连接尝试。 | |
| 危害影响： | 影响OpenSSH:5.7版本(含)到8.4版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.openbsd.org/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145 | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-14145 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202006-1822 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6110)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00643 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。SCP（Secure Copy Protocol）是一个远程文件复制协议。OpenSSH中的SCP客户端实用程序存在安全漏洞。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-468https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://security.netapp.com/advisory/ntap-20190213-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6110 | |
| BID编号： | 106836 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-468 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 信息泄漏漏洞 (CVE-2018-15919)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00645 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.8及之前版本中的auth-gss2.c文件存在信息泄漏漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。\*重点:使用GSS2时会存在漏洞 | |
| 危害影响： | 影响OpenSSH:5.9版本(含)到7.8版本(含) | |
| 解决方案： | 建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201808-902http://www.securityfocus.com/bid/105163http://seclists.org/oss-sec/2018/q3/180https://security.netapp.com/advisory/ntap-20181221-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-15919 | |
| BID编号： | 105163 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201808-902 | |

|  |  |  |
| --- | --- | --- |
| **服务器支持 SSL Insecure Renegotiation(CVE-2009-3555)【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2021-00952 | |
| 端口(服务)： | 800 | |
| 风险描述： | 服务器支持SSL Insecure Renegotiation该漏洞是由于SSL协议设计考虑不周导致的，利用这个漏洞能够在受保护的TLS/SSL连接上引入信息，从而发送流量来欺骗经验证的客户端，造成中间人攻击。 | |
| 危害影响： | 远程攻击者可以利用此漏洞执进行中间人攻击 | |
| 解决方案： | 建议升级openssl来进行修复，openssl-0.98m之后的版本就已经修复了该漏洞，使用了Secure Renegotiation。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2009-3555 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2011-1530 | |
| CNNVD编号： | CNNVD-200911-069 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6109)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00642 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中存在安全漏洞，该漏洞源于程序没有对字符进行编码。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-467https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://usn.ubuntu.com/3885-1/https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6109 | |
| BID编号： | 106843 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-467 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问限制绕过漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-13834 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一套用于安全访问远程计算机的连接工具。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本，scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名，利用该漏洞绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:8.0版本以下版本 | |
| 解决方案： | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20685 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **无效的自签名SSL证书【原理扫描】** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-2022-00050 | |
| 端口(服务)： | 800 | |
| 风险描述： | 此服务的 X.509 证书链未经公认证书颁发机构签名。如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。请注意,此插件不会检查以非自签名、而经未公认证书颁发机构签名的证书结尾的证书链。 | |
| 危害影响： | 如果远程主机为生产环境中的公共主机,这样会使 SSL 的使用无效,因为任何人都可以建立针对远程主机的中间人攻击。 | |
| 解决方案： | 请购买或生成用于此服务的适当证书。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-41617)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10928 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 6.2到8.8之前版本存在安全漏洞。该漏洞源于允许权限提升，因为补充组未按预期初始化。 | |
| 危害影响： | 影响OpenSSH:6.2版本(含)到8.8版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41617 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-41617 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1695 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 输入验证错误漏洞 (CVE-2019-6111)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00644 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中的scp client实用程序存在安全漏洞，该漏洞源于程序错误的验证了对象名称。攻击者可利用该漏洞覆盖文件。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-767https://bugzilla.redhat.com/show\_bug.cgi?id=1677794https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6111 | |
| BID编号： | 106741 | |
| CNVD编号： | CNVD-2019-02499 | |
| CNNVD编号： | CNNVD-201901-767 | |

|  |  |  |
| --- | --- | --- |
| **检测到目标主机加密通信支持的SSL加密算法【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00043 | |
| 端口(服务)： | 800 | |
| 风险描述： | 检测到目标服务加密通信使用的SSL加密算法。 | |
| 危害影响： | 远程攻击者可以利用此漏洞收集信息，方便下一步的攻击行为 | |
| 解决方案： | 该漏洞仅仅是一个信息获取的漏洞，可以不做修复 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | - | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： |  | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 22 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2021-00587 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。 | |
| 危害影响： | 攻击者可以利用该信息进行下一步攻击。 | |
| 解决方案： | 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2008-5161 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2009-12630 | |
| CNNVD编号： | CNNVD-200811-32 | |

## 192.168.7.50

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-28041)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-06510 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。 | |
| 危害影响： | 影响OpenSSH:8.5以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2021-28041http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-202103-527 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-28041 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202103-527 | |

|  |  |  |
| --- | --- | --- |
| **Openssh 命令注入漏洞(CVE-2020-15778)** | | |
| 风险等级： | 高 | |
| 漏洞ID： | SF-0005-02635 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 8.3p1及之前版本中的scp的scp.c文件存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。 | |
| 危害影响： | 影响OpenSSH:8.4p1以下版本(含) | |
| 解决方案： | 可以禁用scp，改用rsync等缓解风险（可能会导致小文件机器内拷贝变慢） | |
| 参考资料： | https://www.openssh.com/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-15778 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202007-1519 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6110)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00643 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。SCP（Secure Copy Protocol）是一个远程文件复制协议。OpenSSH中的SCP客户端实用程序存在安全漏洞。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-468https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://security.netapp.com/advisory/ntap-20190213-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6110 | |
| BID编号： | 106836 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-468 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2021-41617)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10928 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 6.2到8.8之前版本存在安全漏洞。该漏洞源于允许权限提升，因为补充组未按预期初始化。 | |
| 危害影响： | 影响OpenSSH:6.2版本(含)到8.8版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41617 | |
| 协议类型： | - | |
| CVE编号： | CVE-2021-41617 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1695 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞 (CVE-2019-6109)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00642 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中存在安全漏洞，该漏洞源于程序没有对字符进行编码。攻击者可利用该漏洞伪造被显示的文件名。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-467https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txthttps://usn.ubuntu.com/3885-1/https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6109 | |
| BID编号： | 106843 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-467 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2017-15906)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-06522 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.6之前的版本中的sftp-server.c文件的‘process\_open’函数存在安全漏洞，该漏洞源于程序在只读模式下没有正确的阻止写入操作。攻击者可利用该漏洞创建长度为零的文件。 | |
| 危害影响： | 影响OpenSSH:7.6以下版本 | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.openssh.com/txt/release-7.6 | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2017-15906http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201710-1230 | |
| 协议类型： | - | |
| CVE编号： | CVE-2017-15906 | |
| BID编号： | 101552 | |
| CNVD编号： | CNVD-2017-36017 | |
| CNNVD编号： | CNNVD-201710-1230 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 安全漏洞(CVE-2016-20012)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10926 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 8.7之前版本存在安全漏洞，允许远程攻击者怀疑 SSH 服务器知道用户名和公钥的特定组合，以测试这种怀疑是否正确。 发生这种情况是因为仅当该组合对登录会话有效时才会发送质询。 | |
| 危害影响： | 影响OpenSSH:8.7版本(含)以下版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/openssh/openssh-portable/pull/270 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20012 | |
| 协议类型： | - | |
| CVE编号： | CVE-2016-20012 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202109-1073 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH信息泄露漏洞（CVE-2020-14145）** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-10927 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。OpenSSH 5.7至8.3版本的客户端存在信息泄露漏洞。该漏洞产生的原因是OpenSSH客户端中的可观察到的差异会导致算法协商过程中的信息泄露。中间人攻击者可利用该漏洞攻击初始连接尝试。 | |
| 危害影响： | 影响OpenSSH:5.7版本(含)到8.4版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.openbsd.org/security.html | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145 | |
| 协议类型： | - | |
| CVE编号： | CVE-2020-14145 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-202006-1822 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问限制绕过漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-13834 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一套用于安全访问远程计算机的连接工具。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本，scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名，利用该漏洞绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:8.0版本以下版本 | |
| 解决方案： | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2 | |
| 参考资料： | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20685 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 输入验证错误漏洞 (CVE-2019-6111)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00644 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH中的scp client实用程序存在安全漏洞，该漏洞源于程序错误的验证了对象名称。攻击者可利用该漏洞覆盖文件。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201901-767https://bugzilla.redhat.com/show\_bug.cgi?id=1677794https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html | |
| 协议类型： | - | |
| CVE编号： | CVE-2019-6111 | |
| BID编号： | 106741 | |
| CNVD编号： | CNVD-2019-02499 | |
| CNNVD编号： | CNNVD-201901-767 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 信息泄漏漏洞 (CVE-2018-15919)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0005-00645 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.8及之前版本中的auth-gss2.c文件存在信息泄漏漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。\*重点:使用GSS2时会存在漏洞 | |
| 危害影响： | 影响OpenSSH:5.9版本(含)到7.8版本(含) | |
| 解决方案： | 建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://www.openssh.com/ | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201808-902http://www.securityfocus.com/bid/105163http://seclists.org/oss-sec/2018/q3/180https://security.netapp.com/advisory/ntap-20181221-0001/ | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-15919 | |
| BID编号： | 105163 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201808-902 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH 访问控制错误漏洞(CVE-2018-20685)** | | |
| 风险等级： | 中 | |
| 漏洞ID： | SF-0004-50004 | |
| 端口(服务)： | 22 | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。scp Client是其中的一个SCP客户端。OpenSSH 7.9版本中的scp客户端的scp.c文件存在安全漏洞。远程攻击者可借助.文件名或空文件名利用该漏洞造成SSH服务器绕过访问限制。 | |
| 危害影响： | 影响OpenSSH:7.9以下版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.openssh.com/。 | |
| 参考资料： | http://www.securityfocus.com/bid/106531 | |
| 协议类型： | - | |
| CVE编号： | CVE-2018-20685 | |
| BID编号： | 106531 | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-201901-347 | |

|  |  |  |
| --- | --- | --- |
| **ICMP时间戳请求远程日期泄露(CVE-1999-0524)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2022-00076 | |
| 端口(服务)： | 22 | |
| 风险描述： | 远程主机应答ICMP时间戳请求。 这允许攻击者知道在目标计算机上设置的日期，这可以帮助未经身份验证的远程攻击者破坏基于时间的身份验证协议。 从运行Windows Vista / 7/2008/2008 R2的计算机返回的时间戳故意不正确，但通常在实际系统时间的1000秒内。 | |
| 危害影响： | 攻击者可能会利用这些信息,进行信息收集,方便其进行下一步攻击。 | |
| 解决方案： | 暂无解决方案，该插件只是检测主机服务信息，并不检测漏洞信息, 如不使用，可关闭或禁用此服务。 | |
| 参考资料： | http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-199708-003 | |
| 协议类型： | - | |
| CVE编号： | CVE-1999-0524 | |
| BID编号： |  | |
| CNVD编号： |  | |
| CNNVD编号： | CNNVD-199708-003 | |

|  |  |  |
| --- | --- | --- |
| **OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】** | | |
| 风险等级： | 低 | |
| 漏洞ID： | SF-2021-00587 | |
| 端口(服务)： | 22 | |
| 风险描述： | OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。 | |
| 危害影响： | 攻击者可以利用该信息进行下一步攻击。 | |
| 解决方案： | 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| CVE编号： | CVE-2008-5161 | |
| BID编号： |  | |
| CNVD编号： | CNVD-2009-12630 | |
| CNNVD编号： | CNNVD-200811-32 | |

# 参考标准

## 单一系统漏洞风险等级评定标准

|  |  |  |
| --- | --- | --- |
| 危险程度 | 危险值区域 | 危险程度说明 |
| 高 | 7 <= 漏洞风险值<= 10 | 攻击者可以远程执行任意命令或进行远程拒绝服务攻击。 |
| 中 | 4 <= 漏洞风险值< 7 | 攻击者可以利用漏洞攻击其他用户，读写远程系统文件或后台数据库。 |
| 低 | 1 <= 漏洞风险值< 4 | 攻击者可以获取某些系统、文件的信息或冒用身份。 |

## 单一Web漏洞风险等级评定标准

|  |  |  |
| --- | --- | --- |
| 危险程度 | 危险值区域 | 危险程度说明 |
| 高 | 7 <= 漏洞风险值<= 10 | 攻击者可以远程执行任意命令或进行远程拒绝服务攻击。 |
| 中 | 4 <= 漏洞风险值< 7 | 攻击者可以利用漏洞攻击其他用户，读写远程系统文件或后台数据库。 |
| 低 | 1 <= 漏洞风险值< 4 | 攻击者可以获取某些系统、文件的信息或冒用身份。 |

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。

2. 按照风险评估模型计算得到风险值。

3. 注：高、中和低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。

非常危险的资产定义为高风险；比较危险的资产定义为中风险；比较安全和非常安全的资产定义为低风险。