奇安信
新一代网络安全领军者

泸州市生态环境局

主机漏洞扫描分析报告

(保密)

网神信息技术（北京）股份有限公司

2019 年 12 月 10 日

目 录

一. 扫描范围

本次扫描的范围主要对泸州市国控重点污染源自动监控系统（10.194.67.162、10.194.67.163、10.194.67.164、10.194.67.165）、泸州市机动车尾气监管平台系统（10.194.67.166、10.194.67.169、10.194.67.171）、泸州市省控重点污染源自动监控系统（10.194.67.128、10.194.67.115、10.194.67.88、10.194.67.98、10.194.67.85、10.194.67.62）、泸州市企业环境信用评价建设项目管理平台系统（10.194.67.130、10.194.67.131、10.194.67.132、10.194.67.133、10.194.67.134、10.194.67.135）、环境检查移动执法系统（10.194.67.17、10.194.67.79、10.200.200.182）、环境质量在线监测与预警平台系统（10.200.200.25）进行主机漏洞扫描。

二. 扫描目的

通过扫描泸州市生态环境局地址，发现开放服务主机的存在漏洞，并及时触发高危漏洞整改，降低信息安全事件风险。

三. 扫描结果分析

3.1 扫描总体评价

本次扫描漏洞总体情况如下表：

漏洞类型等级	数量	涉及主机数量
严重	0	0
高危	0	0
中危	9	3

主要涉及漏洞问题包括 Apache Tomcat servlet/JSP 容器默认文件等中危问题。

建议业务管理负责人第一时间完成安全问题确认及漏洞修复，并持续完善和优化信息安全管控措施。建议常态化监督安全保障措施的执行落地，确保各类业务尤其是互联网业务的安全运营和可管、可控。

四. 扫描问题详述

4.1 Apache Tomcat servlet/JSP 容器默认文件

威胁等级：中危

问题描述：

示例 JSP 和 Servlet 安装在远程 Apache Tomcat servlet/JSP 容器中。应该删除这些文件，因为它们可能有助于攻击者发现有关远程 Tomcat 安装或主机本身的信息。或者他们本身可能会包含跨站点脚本问题等漏洞。

解决措施：

查看文件并删除不需要的文件。

存在漏洞地址：

Host	Port
10.194.67.163	8080

4.2 SSL 2.0 协议未禁用

威胁等级：中危

问题描述：

远程服务使用 SSL 2.0 进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

解决措施：

禁用 SSL 2.0，使用 TLS 1.0 或更高版本代替。

存在漏洞地址：

Host	Port
10.194.67.165	1433

4.3 SSL 证书签名使用弱强度的哈希算法

威胁等级：中危

问题描述：

远程服务器的 SSL 证书签名使用弱强度的哈希加密算法，例如 MD2、MD4 或者 MD5。这些签名算法显示容易遭到破解。

解决措施：

联系证书认证机构发布新的证书。如果服务器使用自签名证书，则可自己

存在漏洞地址：

Host	Port
10.194.67.165	1433

4.4 允许 SSL 采用中强度加密

威胁等级：中危

问题描述：

远程主机支持 SSL 使用的密码采用中强度解密，即使用的 KEY 解密长度至少 64 位，但少于 112 位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

解决措施：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

存在漏洞地址：

Host	Port
10.194.67.165	1433
10.194.67.17	3901
10.194.67.79	3901

4.5 SSL 证书不被信任

威胁等级：中危

问题描述：

此项服务的 SSL 证书不被信任。

解决措施：

为此项服务购买或生成合适的证书。

存在漏洞地址：

Host	Port
10.194.67.165	1433
10.194.67.17	3901
10.194.67.79	3901

4.6 SSL 自签名证书

威胁等级：中危

问题描述：

服务器所使用的 X.509 签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用 SSL 的效果，因为任何人都可以建立一个中间人攻击远程主机。

解决措施：

购买或者生成被认可的证书。

存在漏洞地址：

Host	Port
10.194.67.165	1433
10.194.67.17	3901
10.194.67.79	3901

4.7 SSLv3 POODLE 安全漏洞

威胁等级：中危

问题描述：

支持 SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为 Padding Oracle On Downloaded Legacy Encryption）可以提取出 SSL 连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

解决措施：

禁用 SSL 3.0。

存在漏洞地址：

Host	Port
10.194.67.165	1433

4.8 DNS 服务器缓存侦听远程信息泄露

威胁等级：中危

问题描述：

远程 DNS 服务器响应没有设置递归位的第三方域的查询。\r\n\r\n 这可能允许远程攻击者确定最近通过此名称服务器解决了哪些域，并且因此了解最近访问了哪些主机。\r\n\r\n 例如，如果攻击者对您的公司是否利用特定金融机构的在线服务感兴趣，他们就可以使用此次攻击来构建关于该金融机构公司使用情况的统计模型。当然，攻击也可以用来查找 B2B 合作伙伴，网络冲浪模式，外部邮件服务器等。\r\n\r\n 注意：如果这是外部网络无法访问的内部 DNS 服务器，攻击将仅限于内部网络。如果支持外部网络访问，这攻击可能包括员工，顾问和访客网络或 WiFi 连接上的潜在用户。

解决措施：

联系 DNS 软件的供应商来修复。http://www.rootsecure.net/content/downdownlo/pdf/dns_cache_snooping.pdf

存在漏洞地址：

Host	Port
10.200.200.182	53
10.200.200.25	53

4.9 mDNS 检测

威胁等级：中危

问题描述：

远程服务了解 Bonjour（也称为 ZeroConf 或 mDNS）协议，允许任何人从远程主机发现信息，例如操作系统类型和确切版本，主机名以及运行的服务列表。\n\n 此插件尝试发现不在引擎所在网段上的主机使用的 mDNS。

解决措施：

如果需要，将进入的流量过滤到 UDP 端口 5353。

存在漏洞地址：

Host	Port
10.194.67.130	5353