# **4.1 主机漏扫统计信息**

## **4.1.4 高危漏洞Top10**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 漏洞名称 | 主机数量 | 漏洞类型 | CVE编号 | 存在主机 |
| 1 | PostgreSQL SQL注入漏洞 | 1 | SQL注入 | CVE-2023-39417 | 192.168.136.155  |
| 2 | PostgreSQL 安全漏洞 | 1 | 其他 | CVE-2023-5869 | 192.168.136.155  |
| 3 | Microsoft SQL Server 远程执行代码漏洞 | 1 | 暂无漏洞类型 | CVE-2015-1762 | 192.168.136.155  |
| 4 | Microsoft SQL Server 远程代码执行漏洞 | 1 | 暂无漏洞类型 | CVE-2015-1763 | 192.168.136.155  |
| 5 | PostgreSQL 加密问题漏洞 | 1 | 加密问题 | CVE-2020-25694 | 192.168.136.155  |
| 6 | PostgreSQL 权限许可和访问控制问题漏洞 | 1 | 权限许可和访问控制问题 | CVE-2022-1552 | 192.168.136.155  |
| 7 | PostgreSQL 安全漏洞 | 1 | 其他 | CVE-2024-0985 | 192.168.136.155  |
| 8 | PostgreSQL 安全漏洞 | 1 | 其他 | CVE-2022-2625 | 192.168.136.155  |
| 9 | PostgreSQL 输入验证错误漏洞 | 1 | 输入验证错误 | CVE-2021-32027 | 192.168.136.155  |
| 10 | PostgreSQL SQL注入漏洞 | 1 | SQL注入 | CVE-2021-23214 | 192.168.136.155  |



## **4.1.8 漏洞详情**

### **4.1.8.1 高危漏洞**

|  |
| --- |
| 【1】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 7.2 |
| CVE编号 | CVE-2023-2454 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202305-1105 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 11版本至15版本存在安全漏洞，该漏洞源于不正确地施加了安全限制，允许远程用户在系统上执行任意代码。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-153-148-1311-1215-and-1120-released-2637/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【2】PostgreSQL SQL注入漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | SQL注入 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.8 |
| CVE编号 | CVE-2023-39417 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202308-1010 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞。攻击者利用该漏洞可以执行任意代码。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/CVE-2023-39417 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【3】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.8 |
| CVE编号 | CVE-2023-5869 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202311-829 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞，该漏洞源于array modification存在整数溢出漏洞。受影响的产品和版本：PostgreSQL 16.1之前的16版本，15.5之前的15版本，14.10之前的14版本，13.13之前的13版本，12.17之前的12版本，11.22之前的11版本。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/download/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【4】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.0 |
| CVE编号 | CVE-2024-0985 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202402-680 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞。攻击者利用该漏洞执行任意 SQL 函数。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/CVE-2024-0985/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【5】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 7.5 |
| CVE编号 | CVE-2024-7348 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202408-631 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞，该漏洞源于pg\_dump的Time-of-check和Time-of-use存在竞争条件，允许攻击者执行任意SQL函数。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/CVE-2024-7348/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【6】Microsoft SQL Server 远程执行代码漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | SqlServer数据库 |
| 漏洞类型 | 暂无漏洞类型 |
| 风险等级 | 高危险 |
| CVSS分值 | 7.1 |
| CVE编号 | CVE-2015-1762 |
| CNCVE编号 | CNCVE-20151762 |
| CNVD编号 | CNVD-2015-04708 |
| CNNVD编号 | CNNVD-201507-425 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统。 Microsoft SQL Server不正确地处理对未初始化内容的内部函数调用时，存在远程代码执行漏洞。攻击者可通过在启用特殊权限设置（如 VIEW SERVER STATE）的受影响的SQL Server上运行特制的查询，利用此漏洞完全控制受影响的系统。以下版本受到影响：Microsoft SQL Server 2008 SP3 和SP4, 2008 R2 SP2和SP3，2012 SP1和SP2，2014。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS15-058 |
| 返回信息 | microsoft:sql\_server:10.50.1600.0 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【7】Microsoft SQL Server 远程代码执行漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | SqlServer数据库 |
| 漏洞类型 | 暂无漏洞类型 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.5 |
| CVE编号 | CVE-2015-1763 |
| CNCVE编号 | CNCVE-20151763 |
| CNVD编号 | CNVD-2015-04706 |
| CNNVD编号 | CNNVD-201507-426 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统。 Microsoft SQL Server不正确地处理对未初始化内容的内部函数调用时，存在远程代码执行漏洞。攻击者可通过运行经特殊设计的查询（旨在从错误地址执行虚拟函数，导致对未初始化的内存进行函数调用），利用此漏洞完全控制受影响的系统。以下版本受到影响：Microsoft SQL Server 2008 SP3 和SP4, 2008 R2 SP2和SP3，2012 SP1和SP2，2014。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS15-058 |
| 返回信息 | microsoft:sql\_server:10.50.1600.0 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【8】PostgreSQL 输入验证错误漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 输入验证错误 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.8 |
| CVE编号 | CVE-2021-32027 |
| CNCVE编号 | CNCVE-202132027 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202105-818 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 中存在输入验证错误漏洞。该漏洞源于网络系统或产品未对输入的数据进行正确的验证。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-133-127-1112-1017-and-9622-released-2210/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【9】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 7.5 |
| CVE编号 | CVE-2020-25696 |
| CNCVE编号 | CNCVE-202025696 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202011-996 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 12.5之前版本存在安全漏洞，该漏洞源于gset 允许覆盖经过特殊处理的变量，gset命令根据查询结果设置psql变量，该命令不区分控制psql行为的变量。攻击者可利用该漏洞执行任意代码作为运行psql的操作系统帐户 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【10】PostgreSQL SQL注入漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | SQL注入 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.8 |
| CVE编号 | CVE-2020-25695 |
| CNCVE编号 | CNCVE-202025695 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202011-1000 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 12.5之前版本中存在SQL注入漏洞，攻击者可利用该漏洞有权在至少一个模式中创建非临时对象，可以以超级用户的身份执行任意SQL函数。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【11】PostgreSQL 加密问题漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 加密问题 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.1 |
| CVE编号 | CVE-2020-25694 |
| CNCVE编号 | CNCVE-202025694 |
| CNVD编号 | CNVD-2020-63992 |
| CNNVD编号 | CNNVD-202011-1004 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 12.5之前版本存在加密问题漏洞，该漏洞源于如果丢弃了与安全性相关的参数（例如channel\_binding，sslmode，requirepeer，gssencmode），则攻击者就有机会完成MITM攻击或观察明文传输。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【12】PostgreSQL SQL注入漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | SQL注入 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.1 |
| CVE编号 | CVE-2021-23214 |
| CNCVE编号 | CNCVE-202123214 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202111-1067 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞，该漏洞源于PostgreSQL处理加密连接的方式造成的。攻击者可利用该漏洞执行MitM攻击。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 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： http://www.postgresql.org/about/news/postgresql-141-135-129-1114-1019-and-9624-released-2349/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【13】PostgreSQL 权限许可和访问控制问题漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 权限许可和访问控制问题 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.8 |
| CVE编号 | CVE-2022-1552 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202205-3080 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在权限许可和访问控制问题漏洞，该漏洞源于autovacuum 功能和多个命令可以逃脱“安全限制操作”沙箱。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-143-137-1211-1116-and-1021-released-2449/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【14】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 高危险 |
| CVSS分值 | 8.0 |
| CVE编号 | CVE-2022-2625 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202208-2831 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞，该漏洞源于攻击者可以利用扩展脚本替换对象来执行代码。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/CVE-2022-2625 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |

### **4.1.8.2 中危漏洞**

|  |
| --- |
| 【1】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 5.4 |
| CVE编号 | CVE-2023-2455 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202305-1104 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 11版本至15版本存在安全漏洞，该漏洞源于应用不正确的策略，允许远程用户绕过实施的安全限制。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-153-148-1311-1215-and-1120-released-2637/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【2】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 4.4 |
| CVE编号 | CVE-2023-5870 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202311-827 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞，该漏洞源于允许角色pg\_signal\_backend表示超级用户进程。受影响的产品和版本：PostgreSQL 16.1之前的16版本，15.5之前的15版本，14.10之前的14版本，13.13之前的13版本，12.17之前的12版本，11.22之前的11版本。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/download/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【3】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 4.3 |
| CVE编号 | CVE-2023-5868 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202311-828 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞，该漏洞源于aggregate函数存在内存泄漏漏洞。受影响的产品和版本：PostgreSQL 16.1之前的16版本，15.5之前的15版本，14.10之前的14版本，13.13之前的13版本，12.17之前的12版本，11.22之前的11版本。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/download/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【4】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 5.0 |
| CVE编号 | CVE-2024-4317 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202405-2255 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL存在安全漏洞。攻击者利用该漏洞可以获取敏感信息。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/support/security/CVE-2024-4317/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【5】Microsoft SQL Server 特权提升漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | SqlServer数据库 |
| 漏洞类型 | 权限许可和访问控制 |
| 风险等级 | 中危险 |
| CVSS分值 | 6.5 |
| CVE编号 | CVE-2015-1761 |
| CNCVE编号 | CNCVE-20151761 |
| CNVD编号 | CNVD-2015-04707 |
| CNNVD编号 | CNNVD-201507-424 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统。 Microsoft SQL Server不适宜地将指针强制转换到不正确的类中时，存在特权提升漏洞。当其凭据允许对受影响的SQL Server数据库的访问时，攻击者可利用此漏洞获得用于查看、更改或删除数据的提升特权；或创新新帐户。以下版本受到影响：Microsoft SQL Server 2008 SP3 和SP4, 2008 R2 SP2和SP3，2012 SP1和SP2，2014。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS15-058 |
| 返回信息 | microsoft:sql\_server:10.50.1600.0 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【6】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 4.3 |
| CVE编号 | CVE-2021-3393 |
| CNCVE编号 | CNCVE-20213393 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202102-1097 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞，攻击者可利用该漏洞可以通过分区约束绕过对数据的访问限制，以获取敏感信息。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://ubuntu.com/security/notices/USN-4735-1 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【7】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 4.3 |
| CVE编号 | CVE-2021-20229 |
| CNCVE编号 | CNCVE-202120229 |
| CNVD编号 | CNVD-2021-14796 |
| CNNVD编号 | CNNVD-202102-1102 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞，攻击者可利用该漏洞可以通过权限绕过对数据的访问限制，以获取敏感信息。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://bugzilla.redhat.com/show\_bug.cgi?id=1925296 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【8】PostgreSQL 缓冲区错误漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 缓冲区错误 |
| 风险等级 | 中危险 |
| CVSS分值 | 6.5 |
| CVE编号 | CVE-2021-32029 |
| CNCVE编号 | CNCVE-202132029 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202105-812 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 中存在缓冲区错误漏洞。攻击者可以读取服务器内存的任意字节。在默认配置中，任何经过身份验证的数据库用户都可以随意创建先决条件对象并完成此攻击。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-133-127-1112-1017-and-9622-released-2210/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【9】PostgreSQL 信息泄露漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 信息泄露 |
| 风险等级 | 中危险 |
| CVSS分值 | 6.5 |
| CVE编号 | CVE-2021-32028 |
| CNCVE编号 | CNCVE-202132028 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202105-815 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 中存在信息泄露漏洞。攻击者可以读取服务器内存的任意字节。在默认配置中，任何经过身份验证的数据库用户都可以随意创建先决条件对象并完成此攻击。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.postgresql.org/about/news/postgresql-133-127-1112-1017-and-9622-released-2210/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【10】PostgreSQL 信息泄露漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 信息泄露 |
| 风险等级 | 中危险 |
| CVSS分值 | 6.5 |
| CVE编号 | CVE-2021-3677 |
| CNCVE编号 | CNCVE-20213677 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202108-1197 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞。本地攻击者可以通过查询PostgreSQL来读取内存片段，以获取敏感信息。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://vigilance.fr/vulnerability/PostgreSQL-information-disclosure-via-Query-36130 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【11】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 中危险 |
| CVSS分值 | 5.9 |
| CVE编号 | CVE-2021-23222 |
| CNCVE编号 | CNCVE-202123222 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202111-1066 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是Postgresql组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞，该漏洞源于PostgreSQL中的libpq进程处理加密连接的方式造成的。攻击者可利用该漏洞窃取可能在会话早期传输的客户端密码或其他机密数据。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 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： http://www.postgresql.org/about/news/postgresql-141-135-129-1114-1019-and-9624-released-2349/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【12】Tyler Odyssey 信任管理问题漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 信任管理问题 |
| 风险等级 | 中危险 |
| CVSS分值 | 5.9 |
| CVE编号 | CVE-2021-43767 |
| CNCVE编号 | CNCVE-202143767 |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202208-3997 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Tyler Technologies Tyler Odyssey是美国Tyler Technologies公司的一个法院和司法软件系统。 Tyler Odyssey 存在安全漏洞，该漏洞源于将未加密字节从中间人传递给客户端 中间攻击者可以向客户端的前几个查询注入错误响应，即使使用了 SSL 证书验证和加密。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 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://github.com/yandex/odyssey/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |

### **4.1.8.3 低危漏洞**

|  |
| --- |
| 【1】PostgreSQL 安全漏洞 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 低危险 |
| CVSS分值 | 3.7 |
| CVE编号 | CVE-2022-41862 |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | CNNVD-202302-999 |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL是PostgreSQL组织的一套自由的对象关系型数据库管理系统。该系统支持大部分SQL标准并且提供了许多其他特性，例如外键、触发器、视图等。 PostgreSQL 存在安全漏洞，该漏洞源于内存泄漏。 |
| 处置优先级 | 优先级低 |
| 排查方法及修复建议 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.suse.com/support/update/announcement/2023/suse-su-20230391-1/ |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |

### **4.1.8.4 信息漏洞**

|  |
| --- |
| 【1】检测到目标主机PostgreSQL服务正在运行 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.155 |
| 简单描述 | PostgreSQL 是一个自由的对象-关系数据库服务器数据库管理系统，它提供了相对其他开放源代码数据库系统比如 MySQL 和 Firebird，和专有系统比如 Oracle、Sybase、IBM 的 DB2 和 Microsoft SQL Server之外的另一种选择。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【2】检测到NoSQL型数据库MongoDB服务正在运行 |
| 影响主机数 | 3 |
| 主机占比 | 38% |
| 漏洞分类 | MongoDB数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | MongoDB是一个介于关系数据库和非关系数据库之间的产品，是非关系数据库当中功能最丰富，最像关系数据库的。他支持的数据结构非常松散，是类似json的bson格式，因此可以存储比较复杂的数据类型。Mongo最大的特点是他支持的查询语言非常强大，其语法有点类似于面向对象的查询语言，几乎可以实现类似关系数据库单表查询的绝大部分功能，而且还支持对数据建立索引。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | mongodb:mongodb |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【3】目标主机MongoDB Web Admin 服务正在运行 |
| 影响主机数 | 3 |
| 主机占比 | 38% |
| 漏洞分类 | MongoDB数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | MongoDB的主要目标是在键/值存储方式（提供了高性能和高度伸缩性）以及传统的RDBMS系统（丰富的功能）架起一座桥梁，集两者的优势于一身。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | mongodb:mongodb |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【4】检测到目标主机SSH服务正在运行 |
| 影响主机数 | 7 |
| 主机占比 | 88% |
| 漏洞分类 | SSH |
| 漏洞类型 | 信息收集 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.144,192.168.136.145,192.168.136.147,192.168.136.149,192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | openbsd:openssh:9.8 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【5】检测到远程主机运行着Microsoft SQL Server  |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | SqlServer数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Microsoft SQL Server 是一个全面的数据库平台，使用集成的商业智能 BI工具提供了企业级的数据管理。Microsoft SQL Server 数据库引擎为关系型数据和结构化数据提供了更安全可靠的存储功能，使您可以构建和管理用于业务的高可用和高性能的数据应用程序。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | microsoft:sql\_server:10.50.1600.0 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【6】Traceroute探测信息 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.155 |
| 简单描述 | 使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者可以利用这些信息来了解目标网络的网络拓扑。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | Here is the route from 192.168.126.61 to 192.168.136.155:\n\n192.168.126.61\n192.168.136.155\n\n |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【7】目标主机MongoDB webadmin服务正在运行 |
| 影响主机数 | 3 |
| 主机占比 | 38% |
| 漏洞分类 | MongoDB数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | MongoDB默认会开启一个HTTP协议的端口提供REST的服务，这个端口是你Server端口加上1000，比如你的Server端口为27017，那么这个HTTP端口就是28017，默认的HTTP端口是数据库状态页面。该web服务会泄露大量数据库信息，并允许攻击者进行非法操作。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | mongodb:mongodb |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【8】探测到Openssh版本信息 |
| 影响主机数 | 7 |
| 主机占比 | 88% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.144,192.168.136.145,192.168.136.147,192.168.136.149,192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。SSH协议族可以用来进行远程控制， 或在计算机之间传送文件。OpenSSH提供了服务端后台程序和客户端工具，用来加密远程控制和文件传输过程中的数据。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | openssh-9.8\n |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【9】远程探测到Microsoft SQL Server正在运行 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | SqlServer数据库 |
| 漏洞类型 | 输入验证 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.155 |
| 简单描述 | Microsoft SQL Server是一款流行的SQL数据库系统 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | microsoft:sql\_server:10.50.1600.0 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【10】检测到Apache ActiveMQ 正在运行 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | 消息中间件 |
| 漏洞类型 | 输入验证 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | - |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.144 |
| 简单描述 | ActiveMQ是一种开源的，实现了JMS1.1规范的，面向消息(MOM)的中间件，为应用程序提供高效的、可扩展的、稳定的和安全的企业级消息通信。ActiveMQ使用Apache提供的授权，任何人都可以对其实现代码进行修改。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | apache:activemq:5.16.7 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【11】检测到远程主机PostgreSQL正在运行 |
| 影响主机数 | 1 |
| 主机占比 | 12% |
| 漏洞分类 | PostgreSQL数据库 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | None |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.155 |
| 简单描述 | 检测到远程主机PostgreSQL正在运行 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 信息收集，无需修复 |
| 返回信息 | postgresql:postgresql:13.0-13.2 |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【12】目标主机SSH服务协议版本可列取 |
| 影响主机数 | 7 |
| 主机占比 | 88% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | None |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.144,192.168.136.145,192.168.136.147,192.168.136.149,192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | SSH协议版本泄露通常会给不法分子进一步渗透提供辅助信息。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 可以通过修改配置屏蔽SSH的banner信息。 |
| 返回信息 | \n |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |
| 【13】目标主机SSH服务加密算法可列取 |
| 影响主机数 | 7 |
| 主机占比 | 88% |
| 漏洞分类 | 其他应用软件 |
| 漏洞类型 | 其他 |
| 风险等级 | 信息 |
| CVSS分值 | 0.0 |
| CVE编号 | - |
| CNCVE编号 | - |
| CNVD编号 | None |
| CNNVD编号 | - |
| 存在主机 | 192.168.136.144,192.168.136.145,192.168.136.147,192.168.136.149,192.168.136.15,192.168.136.151,192.168.136.153 |
| 简单描述 | SSH加密算法泄露通常会给不法分子进一步渗透提供辅助信息。 |
| 处置优先级 | 暂无建议 |
| 排查方法及修复建议 | 可以通过修改配置屏蔽SSH的banner信息。 |
| 返回信息 | Found algorithms\n |
| 漏洞验证状态 |  |
| 漏洞验证返回信息 |  |