**安徽省政务云安全评估报告-主机报表**

**目录**

**1.主机概况**

|  |  |
| --- | --- |
| **主机风险** | **比较危险（5.3分）** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| **IP地址** | 11.64.1.109 |
| **系统版本** | V6.0R04F03SP02 |
| **插件版本** | V6.0R02F01.3300 |
| **配置核查模板版本** | V6.0R04F02.0004 |
| **扫描起始时间** | 2023-11-04 01:56:11 |
| **扫描结束时间** | 2023-11-04 02:01:26 |

 |  |

|  |  |
| --- | --- |
| **漏洞扫描检查模板** | 全部漏洞扫描 |
| **漏洞风险评估分** | 5.3分 |
| **主机风险评估分** | 5.3分 |

 |

**2.漏洞信息**

**2.1 漏洞概况**

漏洞类别： 高危险[0]   中危险[2]   低风险[6]

| **远程扫描** |  |  |  |  |
| --- | --- | --- | --- | --- |
| **端口** | **协议** | **服务** | **漏洞** | **NF已防护** |
| -- | ICMP | -- | * ICMP timestamp请求响应漏洞
 | * -
 |
| -- | UDP | -- | * 允许Traceroute探测
 | * -
 |
| 123 | UDP | ntp | * 检测到目标主机上运行着NTP服务
 | * -
 |
| 10022 | TCP | ssh | * SSH版本信息可被获取
* 探测到SSH服务器支持的算法
 | * -
* -
 |
| 18083 | TCP | http | * Eclipse Jetty 资源管理错误漏洞(CVE-2023-26048)
* Eclipse Jetty 信息泄露漏洞(CVE-2023-26049)
* 可通过HTTP获取远端WWW服务信息
 | * -
* -
* -
 |

**2.2 漏洞详情**

|  |
| --- |
|   Eclipse Jetty 资源管理错误漏洞(CVE-2023-26048) |
|

|  |  |
| --- | --- |
| **详细描述** | Eclipse Jetty是Eclipse基金会的一个开源的、基于Java的Web服务器和Java Servlet容器。Eclipse Jetty 存在资源管理错误漏洞，该漏洞源于当攻击者客户端可能会发送一个大的多部分请求时，会导致服务器抛出OutOfMemoryError。受影响的产品和版本：Jetty-server 9.4.50及之前版本，10.0.13及之前版本，11.0.13及之前版本。 |
| **解决办法** | 厂商补丁: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：https://github.com/eclipse/jetty.project/security/advisories/GHSA-qw69-rqj8-6qw8 |
| **威胁分值** | 5.3 |
| **危险插件** | 否 |
| **发现日期** | 2023-04-18 |
| **CVE编号** | [CVE-2023-26048](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26048) |
| **CNNVD编号** | [CNNVD-202304-1443](https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-202304-1443) |
| **CNCVE编号** | CNCVE-202326048 |

 |
|   Eclipse Jetty 信息泄露漏洞(CVE-2023-26049) |
|

|  |  |
| --- | --- |
| **详细描述** | Eclipse Jetty是Eclipse基金会的一个开源的、基于Java的Web服务器和Java Servlet容器。Eclipse Jetty 存在信息泄露漏洞，该漏洞源于非标准 cookie 解析可能允许攻击者在其他 cookie 中走私 cookie，或者通过篡改 cookie 解析机制来执行意外行为。受影响的产品和版本：Jetty-server 9.4.50及之前版本，10.013及之前版本，11.0.13及之前版本，12.0.0.alpha3及之前版本。 |
| **解决办法** | 厂商补丁: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：https://github.com/eclipse/jetty.project/security/advisories/GHSA-p26g-97m4-6q7c |
| **威胁分值** | 5.3 |
| **危险插件** | 否 |
| **发现日期** | 2023-04-18 |
| **CVE编号** | [CVE-2023-26049](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26049) |
| **CNNVD编号** | [CNNVD-202304-1442](https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-202304-1442) |
| **CNCVE编号** | CNCVE-202326049 |

 |
|   ICMP timestamp请求响应漏洞 |
|   允许Traceroute探测 |
|   检测到目标主机上运行着NTP服务 |
|   SSH版本信息可被获取 |
|   探测到SSH服务器支持的算法 |
|   可通过HTTP获取远端WWW服务信息 |

**3.配置合规信息**

检查项类别：  合规 [0]    不合规 [0]

**4.状态合规信息**

**5.其他信息**

**5.1 远程端口信息**

| **端口** | **协议** | **服务** | **状态** |
| --- | --- | --- | --- |
| 40193 | tcp | unknown | open |
| 36962 | tcp | rmiregistry | open |
| 801 | tcp | http | open |
| 37010 | tcp | unknown | open |
| 10009 | tcp | http | open |
| 12888 | tcp | unknown | open |
| 10022 | tcp | ssh | open |
| 45744 | tcp | unknown | open |
| 42737 | tcp | unknown | open |
| 33766 | tcp | unknown | open |
| 12181 | tcp | unknown | open |
| 18083 | tcp | http | open |
| 38393 | tcp | unknown | open |
| 10008 | tcp | http | open |
| 46472 | tcp | unknown | open |
| 36521 | tcp | unknown | open |
| 19093 | tcp | unknown | open |
| 13888 | tcp | unknown | open |
| 123 | udp | ntp | open |

**5.2 其他信息**

| **其他信息** |
| --- |
| {"application\_layer": "HTTP"} |
| {"service": {"product": "Jetty", "version": "9.4.48"}, "application\_layer": "HTTP", "language": {"product": "Java"}} |

**5.3 安装软件信息**

| **软件名称** | **版本号** |
| --- | --- |
| WWW | Jetty(9.4.48.v20220622); |
| P |  |
| OpenSSH | 8.5 |
| Jetty | 9.4.48.v20220622 |
| SSH | SSH-2.0-OpenSSH\_8.5 |
| SSH Server | SSH-2.0-OpenSSH\_8.5 |

**5.4 端口Banner**

| **端口** | **Banner** |
| --- | --- |
| 10022 | OpenSSH/8.5 |
| 18083 | Jetty/9.4.48.v20220622 |
| 10022 | SSH-2.0-OpenSSH\_8.5 |

**6.对比分析**

**6.1 任务对比分析**

**6.2 漏洞对比分析**

**7.参考标准**

**7.1 单一漏洞风险等级评定标准**

**7.2 单一配置检查项等级评定标准**

**7.3 主机风险等级评定标准**