# 电力监测资产: http://192.168.136.116:8081

|  |  |
| --- | --- |
| 漏洞名称 | PHP缓冲区溢出漏洞(CVE-2023-3824)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-2023-3824 |
| 端口(服务)： | 8081(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP存在安全漏洞，该漏洞源于函数phar\_dir\_read()存在缓冲区溢出漏洞，该漏洞会导致内存损坏或远程代码执行（RCE）。受影响的产品和版本：PHP 8.0.30之前的8.0版本，8.1.22之前的8.1版本，8.2.8之前的8.2版本。 |
| 风险影响： | 受影响的产品和版本：8.0.0<=PHP <8.0.30，8.1.0<=PHP<8.1.22，8.2.0<=PHP <8.2.8 |
| 解决方案： | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb23-30.html |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2023-3824 |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-21006 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx URI处理安全限制绕过漏洞(CVE-2013-4547)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2013-4547 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx是HTTP及反向代理服务器，同时也用作邮件代理服务器，由Igor Sysoev编写。nginx 0.8.41-1.4.3和1.5.x <1.5.7验证包含未转义空间字符的URI时，在实现上存在远程安全限制绕过漏洞，攻击者可利用此漏洞绕过某些安全限制并执行未授权操作。安全通告：http://nginx.org/en/security\_advisories.html<\*来源：Ivan Fratric （ifsecure@gmail.com） 链接：http://secunia.com/advisories/55757/\*> |
| 风险影响： | 影响nginx:0.8.41版本(含)到1.4.3版本(含),1.5.0版本(含)到1.5.7版本 |
| 解决方案： | Nginx-----------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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-11595 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 释放后重利用漏洞(CVE-2016-0746)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0746 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在释放后重利用漏洞。远程攻击者通过CNAME响应处理相关的构造的DNS响应，可造成worker进程崩溃，拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12022 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0742)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0742 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在安全漏洞。通过构造的UDP DNS响应，远程攻击者可造成worker进程资源耗尽，无效指针间接引用，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12023 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 安全漏洞(CVE-2021-23017)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-23017 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | F5 NGINX Controller是美国F5公司的一款用于NGINX的集中式监视和管理平台。该平台支持使用可视化界面管理多个NGINX实例。F5 NGINX Controller存在安全漏洞，该漏洞允许攻击者从DNS服务器伪造UDP数据包造成1-byte的内存覆盖，导致工作进程崩溃或潜在的其他影响。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.20.1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.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 参考资料： | https://www.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12904 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 输入验证错误漏洞(CVE-2017-20005)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2017-20005 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx是美国Nginx公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。NGINX在1.13.6之前存在安全漏洞，该漏洞源于当autoindex模块遇到这个文件时，会导致一个整数溢出。 |
| 风险影响： | 影响nginx:1.13.6以下版本 |
| 解决方案： | 下载更高版本进行升级，下载链接：http://nginx.org/en/download.html，升级方法链接：https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 参考资料： | http://nginx.org/en/download.html https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12905 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 信任管理问题漏洞(CVE-2021-3618)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-3618 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | 此插件基于nginx版本检测，有可能误报。\nNginx是美国F5公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器，在BSD-like协议下发行。 \nNginx存在信任管理问题漏洞，该漏洞源于存在 ALPACA（应用层协议内容混淆）攻击，这会破坏TLS的身份验证，并且可能会发生跨协议攻击。 |
| 风险影响： | 影响Nginx:1.21.0以下版本 |
| 解决方案： | 厂商升级:Nginx-----目前厂商已经发布了新版本以修复这个安全问题，请到厂商的主页下载：下载链接：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-16917 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP 缓冲区错误漏洞(CVE-2022-31630)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2022-31630 |
| 端口(服务)： | 8081(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP 8.1.12之前版本存在安全漏洞，该漏洞源于攻击者可以通过imageloadfont强制读取无效内存地址，以触发拒绝服务或获取敏感信息。 |
| 风险影响： | 影响PHP:7.4.0版本(含)到7.4.33版本,8.0.0版本(含)到8.0.25版本,8.1.0版本(含)到8.1.12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.php.net/ChangeLog-8.php#8.0.25 |
| 参考资料： | http://www.php.net |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-15323 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx SSL会话固定漏洞(CVE-2014-3616)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2014-3616 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx　0.5.6－1.7.4版本在实现上存在会话固定漏洞，攻击者可利用此漏洞劫持任意会话或访问敏感信息。<\*来源：Antoine Delignat-Lavaud \*> |
| 风险影响： | 影响nginx:0.5.6版本(含)到1.7.4版本(含) |
| 解决方案： | Nginx-----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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12019 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0747)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0747 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver未正确限制CNAME解析度。通过任意名称解析相关矢量，远程攻击者可造成worker进程资源耗尽，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12021 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 环境问题漏洞(CVE-2020-12440)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2020-12440 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | NGINX是美国NGINX公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。 NGINX中存在环境问题漏洞。攻击者可利用该漏洞进行缓存投毒，劫持凭证或绕过安全保护。 |
| 风险影响： | 影响nginx:1.18.0以下版本(含) |
| 解决方案： | 厂商补丁:https://www.nginx.com/ |
| 参考资料： | https://www.nginx.com/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12944 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 未授权访问漏洞(CVE-2019-20372)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-20372 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx 1.17.7之前版本中存在未授权访问漏洞。攻击者可利用该漏洞读取未授权的Web页面。 |
| 风险影响： | Nginx<1.17.7 |
| 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://nginx.org/en/CHANGES |
| 参考资料： | https://usn.ubuntu.com/4235-1/ https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2020\_11519&lang=ZH-CN |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-13810 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP password\_verify失效认证漏洞通告（CVE-2023-0567）【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-0567 |
| 端口(服务)： | 8081(PHP) |
| 风险描述： | PHP（全称：PHP：Hypertext Preprocessor，即“超文本预处理器”）是一种开源的计算机脚本语言，适用于Web开发并可嵌入HTML中，password\_verify() 函数用于验证密码是否和散列值匹配。近日，新华三攻防实验室威胁预警团队监测到PHP官方发布了安全公告，修复了一个存在于password\_verify中的失效认证漏洞（CVE-2023-0567），且漏洞利用代码已公开，攻击者利用该漏洞可导致应用程序允许任何密码都有效。\n影响范围：\n8.1.x <= PHP <8.1.16\n8.2.x <= PHP <8.2.23\n8.0.x <= PHP <8.0.28\n参考链接：https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4 |
| 风险影响： | 影响PHP:8.1.0版本(含)到8.1.16版本,8.2版本(含)到8.2.3版本,8.0版本(含)到8.0.28版本 |
| 解决方案： | 厂商补丁:目前官方已修复该漏洞，受影响用户可以升级更新到安全版本。官方下载链接：https://github.com/php/php-src/tags |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-17018 |

# 机房动环资产: 192.168.103.201

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH sshd 拒绝服务漏洞 (CVE-2016-10708)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-10708 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。sshd是其中的一个独立守护进程。OpenSSH 7.4之前版本中的sshd存在安全漏洞。远程攻击者可借助乱序的NEWKEYS消息利用该漏洞造成拒绝服务（空指针逆向引用和守护进程崩溃）。 |
| 风险影响： | 影响OpenSSH:7.4之前的版本 |
| 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/releasenotes.html |
| 参考资料： | http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html https://security.netapp.com/advisory/ntap-20180423-0003/ https://www.openssh.com/releasenotes.html |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-00641 |

|  |  |
| --- | --- |
| 漏洞名称 | Openssh 命令注入漏洞(CVE-2020-15778)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2020-15778 |
| 端口(服务)： | 22(OpenSSH) |
| 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。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。 |
| 风险影响： | 影响OpenSSH:8.3p1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），修复方案参考：https://wenku.baidu.com/view/b41e84ca0a75f46527d3240c844769eae009a3e3.html?\_wkts\_=1668080327922 |
| 参考资料： | https://www.openssh.com/ https://wenku.baidu.com/view/b41e84ca0a75f46527d3240c844769eae009a3e3.html |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-02635 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 远程代码执行漏洞(CVE-2016-10009)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-10009 |
| 端口(服务)： | 22(OpenSSH) |
| 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 7.4之前版本中的ssh-agent的ssh-agent.c文件存在代码问题漏洞。远程攻击者可通过控制转发的agent-socket利用该漏洞执行任意本地PKCS＃11模块。 |
| 风险影响： | 影响OpenSSH:7.4以下版本 |
| 解决方案： | 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://www.openssh.com/txt/release-7.4，或者下载更高版本进行升级，下载链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | http://www.openssh.com/txt/release-7.4 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-06974 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 远程权限提升漏洞(CVE-2016-10010)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-10010 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。sshd是其中的一个独立守护进程。OpenSSH 7.4之前的版本中的sshd存在安全漏洞。本地攻击者可利用该漏洞获取权限。 |
| 风险影响： | 影响OpenSSH:7.4以下版本 |
| 解决方案： | 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://www.openssh.com/txt/release-7.4，或者下载更高版本进行升级，下载链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | https://doc.pfsense.org/index.php/2.3.3\_New\_Features\_and\_Changes http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-06975 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全限制绕过漏洞(CVE-2016-10012)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-10012 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。sshd是其中的一个独立守护进程。OpenSSH 7.4之前的版本中的sshd的共享内存管理器存在安全漏洞。本地攻击者可通过访问沙箱privilege-separation进程利用该漏洞获取权限。 |
| 风险影响： | 影响OpenSSH:7.4以下版本 |
| 解决方案： | 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/openbsd/src/commit/3095060f479b86288e31c79ecbc5131a66bcd2f9，或者下载更高版本进行升级，下载链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | https://support.apple.com/en-us/HT207615 https://lists.apple.com/archives/security-announce/2017/Mar/msg00004.html https://httpoxy.org https://github.com/openbsd/src/commit/3095060f479b86288e31c79ecbc5131a66bcd2f9 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-06977 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH do\_setup\_env函数权限提升漏洞(CVE-2015-8325)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2015-8325 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | OpenSSH是SSH协议的开源实现。OpenSSH 7.2p2之前版本, sshd/ session.c/ do\_setup\_env函数存在安全漏洞, 启用了UseLogin功能且PAM配置为读取用户主目录内的 .pam\_environment文件后, 本地用户通过触发/bin/login程序构造的环境, 可提升其权限。 |
| 风险影响： | 影响OpenSSH:7.2p2以下版本(含) |
| 解决方案： | 厂商补丁:OpenSSH-------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://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html、https://security-tracker.debian.org/tracker/CVE-2015-8325、https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755 |
| 参考资料： | https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html https://security-tracker.debian.org/tracker/CVE-2015-8325 https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-11585 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH auth\_password函数拒绝服务漏洞(CVE-2016-6515)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-6515 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | OpenSSH是SSH协议的开源实现。OpenSSH 7.3之前版本，sshd/auth-passwd.c/auth\_password函数未限制密码验证中的密码长度，远程攻击者通过较长的字符串，利用此漏洞可造成拒绝服务。 |
| 风险影响： | 影响OpenSSH:7.3以下版本 |
| 解决方案： | 厂商补丁:OpenSSH-------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：http://openwall.com/lists/oss-security/2016/08/01/2或者https://github.com/openssh/openssh-portable/commit/fcd135c9df440bcd2d5870405ad3311743d78d97 |
| 参考资料： | http://www.openssh.com/txt/release-7.3 http://openwall.com/lists/oss-security/2016/08/01/2 https://github.com/openssh/openssh-portable/commit/fcd135c9df440bcd2d5870405ad3311743d78d97 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-11586 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2016-1908)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-1908 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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OpenSSH客户端没有正确为不可信的X11转发生成身份验证cookie。攻击者可利用该漏洞与本地X服务器建立可信连接。 |
| 风险影响： | 影响OpenSSH:7.1p2以下版本 |
| 解决方案： | 厂商补丁：OpenSSH-------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：http://www.openssh.com/txt/release-7.2或者下载更高版本进行升级，下载链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | http://www.openssh.com/txt/release-7.2 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-12165 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2021-41617)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-41617 |
| 端口(服务)： | 22(OpenSSH) |
| 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。 |
| 风险影响： | 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://bugzilla.suse.com/show\_bug.cgi?id=1190975 或者下载更高版本进行升级，下载链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ 升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | https://bugzilla.suse.com/show\_bug.cgi?id=1190975 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-13648 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH ssh-agent远程代码执行漏洞(CVE-2023-38408)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-38408 |
| 端口(服务)： | 22(OpenSSH) |
| 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 的 ssh-agent 中存在了一个远程代码执行漏洞。此漏洞允许远程攻击者在存在漏洞的 OpenSSH的 forwarded ssh-agent 代理上执行任意命令。 |
| 风险影响： | 影响openssh: 5.5版本（含）到9.3.p1版本（含） |
| 解决方案： | 该漏洞在OpenSSH 9.3p2版本中已得到修复。建议用户升级到最新版本。对于 OpenBSD，发布了一个勘误补丁来修复此问题。  链接如下：https://www.openssh.com/releasenotes.html  https://www.openbsd.org/errata.html |
| 参考资料： | https://blog.qualys.com/vulnerabilities-threat-research/2023/07/19/cve-2023-38408-remote-code-execution-in-opensshs-forwarded-ssh-agent |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-16132 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH roaming\_common.c堆缓冲区溢出漏洞(CVE-2016-0778)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0778 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | OpenSSH是SSH协议的开源实现。\nOpenSSH 5.x, 6.x, 7.1p2之前的7.x版本，启用了某些代理及转发选项后，roaming\_common.c内的函数roaming\_read及roaming\_write未正确保留连接文件描述符，这可使远程服务器造成拒绝服务（堆缓冲区溢出）。 |
| 风险影响： | 影响OpenSSH:5.0版本(含)到7.2p2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.openwall.com/lists/oss-security/2023/03/15/8http://www.openssh.com/txt/release-7.1p2 |
| 参考资料： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-16932 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 信息泄漏漏洞 (CVE-2023-51385)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-51385 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | OpenSSH 是使用 SSH 协议进行远程登录的连接工具。在OpenSSH 9.6版本之前的ssh中，如果用户名或主机名中含有shell元字符（如 | ‘ “等），并且ssh\_config中ProxyCommand、LocalCommand指令或”match exec”谓词通过%u、%h或类似的扩展标记引用用户或主机名时，可能会发生命令注入。Git未禁止用户或主机名中的shell元字符，存储库可能包含一个带有shell元字符的子模块用户或主机名，可能导致产生命令注入漏洞。 |
| 风险影响： | 影响OpenSSH:影响9.6以下版本 |
| 解决方案： | 将 openssh 升级至 9.6 及以上版本 |
| 参考资料： | https://www.openssh.com/txt/release-9.6 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-17090 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH ssh/kex.c 拒绝服务漏洞(CVE-2016-8858)【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-8858 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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 6.x版本和7.x至7.3版本中的kex.c文件的‘kex\_input\_kexinit’函数存在拒绝服务漏洞。远程攻击者可通过发送许多复制的KEXINIT请求利用该漏洞造成拒绝服务。注意：第三方报告称不将OpenSSH upstream视为安全漏洞。 |
| 风险影响： | OpenSSH 如下版本将受影响：6.8,6.9,7.0,7.1,7.2,7.3 |
| 解决方案： | 升级至 OpenSSH 最新版本：http://www.openssh.com/ |
| 参考资料： | http://www.ibm.com/support/docview.wss?uid=swg22017294 https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201610-679 http://www.ibm.com/support/docview.wss?uid=ibm10885602 http://www.ibm.com/support/docview.wss?uid=ibm10885606 |
| 协议类型： | - |
| 风险举证: |  |
| 漏洞ID： | SF-2019-00287 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 访问控制错误漏洞(CVE-2018-20685)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2018-20685 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。 |
| 风险影响： | 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： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0004-50004 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 访问控制错误漏洞 (CVE-2019-6109)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-6109 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。 |
| 风险影响： | 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： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201901-467 https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt https://usn.ubuntu.com/3885-1/ https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-00642 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 访问控制错误漏洞 (CVE-2019-6110)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-6110 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。 |
| 风险影响： | 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： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201901-468 https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt https://security.netapp.com/advisory/ntap-20190213-0001/ |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-00643 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 输入验证错误漏洞 (CVE-2019-6111)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-6111 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。 |
| 风险影响： | 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： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201901-767 https://bugzilla.redhat.com/show\_bug.cgi?id=1677794 https://lists.debian.org/debian-lts-announce/2019/03/msg00030.html |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-00644 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 信息泄漏漏洞 (CVE-2018-15919)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2018-15919 |
| 端口(服务)： | 22(OpenSSH) |
| 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 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 |
| 风险影响： | 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： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201808-902 http://seclists.org/oss-sec/2018/q3/180 https://security.netapp.com/advisory/ntap-20181221-0001/ |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-00645 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 本地信息泄露漏洞(CVE-2016-10011)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-10011 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。sshd是其中的一个独立守护进程。OpenSSH 7.4之前的版本中的sshd的authfile.c文件中存在安全漏洞。本地攻击者可通过访问privilege-separated子进程利用该漏洞获取敏感的私钥信息。 |
| 风险影响： | 影响OpenSSH:7.4以下版本 |
| 解决方案： | 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://www.openssh.com/txt/release-7.4, 下载高版本链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | http://www.openssh.com/txt/release-7.4 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-06976 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH SSH守护进程安全漏洞(CVE-2016-6210)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-6210 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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 SSH守护进程中存在安全漏洞，远程攻击者可通过发送长密码利用该漏洞接收不存在用户较短的响应时间。 |
| 风险影响： | 影响OpenSSH:7.3以下版本 |
| 解决方案： | 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://www.openssh.com/txt/release-7.3, 下载高版本链接：http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/，升级方法链接：https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 参考资料： | https://www.openssh.com/txt/release-7.3 http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ https://blog.csdn.net/qq\_29768197/article/details/125048720 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-11791 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2017-15906)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2017-15906 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。 |
| 风险影响： | 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： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-11886 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH <=7.2p1 xauth命令注入漏洞(CVE-2016-3115)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-3115 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | OpenSSH是SSH协议的开源实现。OpenSSH <=7.2p1在实现上存在xauth命令注入漏洞，可导致绕过forced-command及/bin/false。<\*来源：tintinweb \*> |
| 风险影响： | 影响OpenSSH:7.1p2以下版本 |
| 解决方案： | 厂商补丁：OpenSSH-------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：[1] http://www.openssh.com/[2] https://github.com/openssh/openssh-portable/blob/5a0fcb77287342e2fc2ba1cee79b6af108973dc2/session.c#L1388[3] https://github.com/openssh/openssh-portable/blob/19bcf2ea2d17413f2d9730dd2a19575ff86b9b6a/clientloop.c#L376[4] http://linux.die.net/man/1/xauth[5] http://www.openssh.com/txt/x11fwd.adv |
| 参考资料： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-12164 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2016-20012)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-20012 |
| 端口(服务)： | 22(OpenSSH) |
| 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。 |
| 风险影响： | 影响OpenSSH: 8.7及之前版本 |
| 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： | 链接：https://github.com/openssh/openssh-portable/pull/270 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-20012 |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-13647 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH信息泄露漏洞（CVE-2020-14145）【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2020-14145 |
| 端口(服务)： | 22(OpenSSH) |
| 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 5.7版本至8.6版本的客户端中存在信息泄露漏洞。攻击者可利用该漏洞获取信息。 |
| 风险影响： | 影响OpenSSH:5.7版本(含)到8.6版本(含) |
| 解决方案： |  |
| 参考资料： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-13649 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH client信息泄露漏洞(CVE-2016-0777)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0777 |
| 端口(服务)： | 22(OpenSSH) |
| 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是SSH协议的开源实现。OpenSSH 5.x, 6.x, 7.1p2之前的7.x版本，client内roaming\_common.c的函数resend\_bytes存在安全漏洞，远程攻击者通过请求传输整个缓冲区，利用此漏洞可获取进程内存的敏感信息。 |
| 风险影响： | 影响OpenSSH:5.0版本(含)到7.1.p2版本 |
| 解决方案： | 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://www.openssh.com/txt/release-7.1p2 |
| 参考资料： |  |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-14256 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2023-51384)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-51384 |
| 端口(服务)： | 22(OpenSSH) |
| 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）是加拿大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 9.6之前版本存在安全漏洞，该漏洞源于当在添加PKCS11托管私钥的过程中指定目标约束时，这些约束仅应用于第一个密钥。 |
| 风险影响： | 影响OpenSSH:9.6版本以下版本 |
| 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://www.openssh.com/txt/release-9.6 |
| 参考资料： | https://www.openssh.com |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-17307 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2023-51767)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-51767 |
| 端口(服务)： | 22(OpenSSH) |
| 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）是加拿大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 9.6及之前版本存在安全漏洞，该漏洞源于当使用常见类型的DRAM时，mm\_answer\_authpassword中已验证的整数值不能抵抗单个比特的翻转，导致攻击者可以绕过身份验证。 |
| 风险影响： | 影响OpenSSH:9.6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://www.openssh.com/txt/release-9.6 |
| 参考资料： | https://www.openssh.com |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-17308 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 安全漏洞(CVE-2023-48795)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-48795 |
| 端口(服务)： | 22(OpenSSH) |
| 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）是加拿大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 9.6之前版本存在安全漏洞，该漏洞源于允许远程攻击者绕过完整性检查，从而省略某些数据包。 |
| 风险影响： | 影响OpenSSH:9.6版本以下版本 |
| 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://www.openssh.com/openbsd.html |
| 参考资料： | https://www.openssh.com |
| 协议类型： | ssh |
| 风险举证: | OpenSSH: 7.1 |
| 漏洞ID： | SF-0005-21000 |

|  |  |
| --- | --- |
| 漏洞名称 | OpenSSH 用户名枚举漏洞(CVE-2018-15473)【原理扫描】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2018-15473 |
| 端口(服务)： | 22(OpenSSH) |
| 风险描述： | 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。由于使用不存在的用户名和存在的用户名将返回不同的信息，该特性将能够被用来进行用户名枚举，并可能使用结果进行更进一步攻击。 |
| 风险影响： | 影响<=7.7的版本 |
| 解决方案： | 升级至 OpenSSH 最新版本：http://www.openssh.com/ |
| 参考资料： | https://blog.csdn.net/gh0stf1re/article/details/108641707 |
| 协议类型： | - |
| 风险举证: | 使用不存在的用户名（随机生成）和存在的用户名（root）尝试连接将返回不同的信息，该特性将能够被用来进行用户名枚举，并可能使用结果进行更进一步攻击。 |
| 漏洞ID： | SF-2019-00163 |

# 动环资产: 192.168.133.202

|  |  |
| --- | --- |
| 漏洞名称 | SNMP代理默认社区名称（public）(CVE-1999-0517)【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-1999-0517 |
| 端口(服务)： | 161(unknown) |
| 风险描述： | 可以获得远程SNMP服务器的默认社区名。攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 风险影响： | 攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 解决方案： | 如果您不使用远程主机上的SNMP服务，则禁用它, 要么过滤进入该端口的UDP数据包，要么更改默认的社区字符串：https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 参考资料： | https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 协议类型： | udp |
| 风险举证: | The remote SNMP server replies to the following default community string : public |
| 漏洞ID： | SF-0006-01784 |

# 动环资产: 192.168.133.203

|  |  |
| --- | --- |
| 漏洞名称 | SNMP代理默认社区名称（public）(CVE-1999-0517)【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-1999-0517 |
| 端口(服务)： | 161(unknown) |
| 风险描述： | 可以获得远程SNMP服务器的默认社区名。攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 风险影响： | 攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 解决方案： | 如果您不使用远程主机上的SNMP服务，则禁用它, 要么过滤进入该端口的UDP数据包，要么更改默认的社区字符串：https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 参考资料： | https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 协议类型： | udp |
| 风险举证: | The remote SNMP server replies to the following default community string : public |
| 漏洞ID： | SF-0006-01784 |

# 动环资产: 192.168.133.205

|  |  |
| --- | --- |
| 漏洞名称 | SNMP代理默认社区名称（public）(CVE-1999-0517)【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-1999-0517 |
| 端口(服务)： | 161(unknown) |
| 风险描述： | 可以获得远程SNMP服务器的默认社区名。攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 风险影响： | 攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 解决方案： | 如果您不使用远程主机上的SNMP服务，则禁用它, 要么过滤进入该端口的UDP数据包，要么更改默认的社区字符串：https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 参考资料： | https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 协议类型： | udp |
| 风险举证: | The remote SNMP server replies to the following default community string : public |
| 漏洞ID： | SF-0006-01784 |

# 动环资产: 192.168.133.206

|  |  |
| --- | --- |
| 漏洞名称 | SNMP代理默认社区名称（public）(CVE-1999-0517)【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-1999-0517 |
| 端口(服务)： | 161(unknown) |
| 风险描述： | 可以获得远程SNMP服务器的默认社区名。攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 风险影响： | 攻击者可以使用这些信息来获得关于远程主机的更多信息，或者更改远程系统的配置(如果默认社区允许这样的修改)。 |
| 解决方案： | 如果您不使用远程主机上的SNMP服务，则禁用它, 要么过滤进入该端口的UDP数据包，要么更改默认的社区字符串：https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 参考资料： | https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-1999-0517 |
| 协议类型： | udp |
| 风险举证: | The remote SNMP server replies to the following default community string : public |
| 漏洞ID： | SF-0006-01784 |

# 电力监测资产: 192.168.136.116

|  |  |
| --- | --- |
| 漏洞名称 | PHP缓冲区溢出漏洞(CVE-2023-3824)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-2023-3824 |
| 端口(服务)： | 80(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP存在安全漏洞，该漏洞源于函数phar\_dir\_read()存在缓冲区溢出漏洞，该漏洞会导致内存损坏或远程代码执行（RCE）。受影响的产品和版本：PHP 8.0.30之前的8.0版本，8.1.22之前的8.1版本，8.2.8之前的8.2版本。 |
| 风险影响： | 受影响的产品和版本：8.0.0<=PHP <8.0.30，8.1.0<=PHP<8.1.22，8.2.0<=PHP <8.2.8 |
| 解决方案： | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb23-30.html |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2023-3824 |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-21006 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP缓冲区溢出漏洞(CVE-2023-3824)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | CVE-2023-3824 |
| 端口(服务)： | 8081(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP存在安全漏洞，该漏洞源于函数phar\_dir\_read()存在缓冲区溢出漏洞，该漏洞会导致内存损坏或远程代码执行（RCE）。受影响的产品和版本：PHP 8.0.30之前的8.0版本，8.1.22之前的8.1版本，8.2.8之前的8.2版本。 |
| 风险影响： | 受影响的产品和版本：8.0.0<=PHP <8.0.30，8.1.0<=PHP<8.1.22，8.2.0<=PHP <8.2.8 |
| 解决方案： | 厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb23-30.html |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2023-3824 |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-21006 |

|  |  |
| --- | --- |
| 漏洞名称 | Memcached 未授权访问漏洞【原理扫描】 |
| 风险等级： | 高 |
| 高可利用： | 是 |
| CVE编号： | - |
| 端口(服务)： | 11211(Memcached) |
| 风险描述： | Memcached 端口对外开放并且没有配置认证选项，未授权用户可直接获取数据库中所有信息，造成严重的信息泄露。 |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 |
| 解决方案： | 增加Memcached 的认证配置 1.配置访问控制,通过安全组规则或防火墙配置访问控制规则， 2.—bind 制定监听IP,最小化权限运行,修改默认端口，如果Memcached没有在外网开放的必要，可在Memcached启动的时候指定绑定的ip地址为 127.0.0.1，使用普通权限账号运行。 |
| 参考资料： | https://www.freesion.com/article/9220615261/ http://memcached.org/ https://www.mediawiki.org/wiki/Memcached |
| 协议类型： | - |
| 风险举证: | 通过socket发送如下数据：  b'stats\n'  收到如下响应:  b'STAT pid 5144\r\nSTAT uptime 180484\r\nSTAT time 1723895273\r\nSTAT version 1.2.1\r\nSTAT pointer\_size 32\r\nSTAT curr\_items 307\r\nSTAT total\_items 12396895\r\nSTAT bytes 102897\r\nSTAT curr\_connections 3\r\nSTAT total\_connections 6245174\r\nSTAT connection\_structures 14\r\nSTAT cmd\_get 87737487\r\nSTAT cmd\_set 12396887\r\nSTAT get\_hits 87537290\r\nSTAT get\_misses 200197\r\nSTAT bytes\_read 18646927580\r\nSTAT bytes\_written 208186293616\r\nSTAT limit\_maxbytes 67108864\r\nEND\r\n' |
| 漏洞ID： | SF-2021-00583 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx URI处理安全限制绕过漏洞(CVE-2013-4547)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2013-4547 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | Nginx是HTTP及反向代理服务器，同时也用作邮件代理服务器，由Igor Sysoev编写。nginx 0.8.41-1.4.3和1.5.x <1.5.7验证包含未转义空间字符的URI时，在实现上存在远程安全限制绕过漏洞，攻击者可利用此漏洞绕过某些安全限制并执行未授权操作。安全通告：http://nginx.org/en/security\_advisories.html<\*来源：Ivan Fratric （ifsecure@gmail.com） 链接：http://secunia.com/advisories/55757/\*> |
| 风险影响： | 影响nginx:0.8.41版本(含)到1.4.3版本(含),1.5.0版本(含)到1.5.7版本 |
| 解决方案： | Nginx-----------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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-11595 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 释放后重利用漏洞(CVE-2016-0746)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0746 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在释放后重利用漏洞。远程攻击者通过CNAME响应处理相关的构造的DNS响应，可造成worker进程崩溃，拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12022 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0742)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0742 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在安全漏洞。通过构造的UDP DNS响应，远程攻击者可造成worker进程资源耗尽，无效指针间接引用，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12023 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 安全漏洞(CVE-2021-23017)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-23017 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | F5 NGINX Controller是美国F5公司的一款用于NGINX的集中式监视和管理平台。该平台支持使用可视化界面管理多个NGINX实例。F5 NGINX Controller存在安全漏洞，该漏洞允许攻击者从DNS服务器伪造UDP数据包造成1-byte的内存覆盖，导致工作进程崩溃或潜在的其他影响。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.20.1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.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 参考资料： | https://www.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12904 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 输入验证错误漏洞(CVE-2017-20005)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2017-20005 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | Nginx是美国Nginx公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。NGINX在1.13.6之前存在安全漏洞，该漏洞源于当autoindex模块遇到这个文件时，会导致一个整数溢出。 |
| 风险影响： | 影响nginx:1.13.6以下版本 |
| 解决方案： | 下载更高版本进行升级，下载链接：http://nginx.org/en/download.html，升级方法链接：https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 参考资料： | http://nginx.org/en/download.html https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12905 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 信任管理问题漏洞(CVE-2021-3618)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-3618 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | 此插件基于nginx版本检测，有可能误报。\nNginx是美国F5公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器，在BSD-like协议下发行。 \nNginx存在信任管理问题漏洞，该漏洞源于存在 ALPACA（应用层协议内容混淆）攻击，这会破坏TLS的身份验证，并且可能会发生跨协议攻击。 |
| 风险影响： | 影响Nginx:1.21.0以下版本 |
| 解决方案： | 厂商升级:Nginx-----目前厂商已经发布了新版本以修复这个安全问题，请到厂商的主页下载：下载链接：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-16917 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx URI处理安全限制绕过漏洞(CVE-2013-4547)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2013-4547 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx是HTTP及反向代理服务器，同时也用作邮件代理服务器，由Igor Sysoev编写。nginx 0.8.41-1.4.3和1.5.x <1.5.7验证包含未转义空间字符的URI时，在实现上存在远程安全限制绕过漏洞，攻击者可利用此漏洞绕过某些安全限制并执行未授权操作。安全通告：http://nginx.org/en/security\_advisories.html<\*来源：Ivan Fratric （ifsecure@gmail.com） 链接：http://secunia.com/advisories/55757/\*> |
| 风险影响： | 影响nginx:0.8.41版本(含)到1.4.3版本(含),1.5.0版本(含)到1.5.7版本 |
| 解决方案： | Nginx-----------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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-11595 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 释放后重利用漏洞(CVE-2016-0746)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0746 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在释放后重利用漏洞。远程攻击者通过CNAME响应处理相关的构造的DNS响应，可造成worker进程崩溃，拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12022 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0742)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0742 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver存在安全漏洞。通过构造的UDP DNS响应，远程攻击者可造成worker进程资源耗尽，无效指针间接引用，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12023 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 安全漏洞(CVE-2021-23017)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-23017 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | F5 NGINX Controller是美国F5公司的一款用于NGINX的集中式监视和管理平台。该平台支持使用可视化界面管理多个NGINX实例。F5 NGINX Controller存在安全漏洞，该漏洞允许攻击者从DNS服务器伪造UDP数据包造成1-byte的内存覆盖，导致工作进程崩溃或潜在的其他影响。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.20.1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.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 参考资料： | https://www.nginx.com/blog/updating-nginx-dns-resolver-vulnerability-cve-2021-23017/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12904 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 输入验证错误漏洞(CVE-2017-20005)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2017-20005 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx是美国Nginx公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。NGINX在1.13.6之前存在安全漏洞，该漏洞源于当autoindex模块遇到这个文件时，会导致一个整数溢出。 |
| 风险影响： | 影响nginx:1.13.6以下版本 |
| 解决方案： | 下载更高版本进行升级，下载链接：http://nginx.org/en/download.html，升级方法链接：https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 参考资料： | http://nginx.org/en/download.html https://blog.csdn.net/qq\_46023525/article/details/122079552 |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12905 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 信任管理问题漏洞(CVE-2021-3618)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2021-3618 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | 此插件基于nginx版本检测，有可能误报。\nNginx是美国F5公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器，在BSD-like协议下发行。 \nNginx存在信任管理问题漏洞，该漏洞源于存在 ALPACA（应用层协议内容混淆）攻击，这会破坏TLS的身份验证，并且可能会发生跨协议攻击。 |
| 风险影响： | 影响Nginx:1.21.0以下版本 |
| 解决方案： | 厂商升级:Nginx-----目前厂商已经发布了新版本以修复这个安全问题，请到厂商的主页下载：下载链接：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-16917 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP 缓冲区错误漏洞(CVE-2022-31630)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2022-31630 |
| 端口(服务)： | 80(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP 8.1.12之前版本存在安全漏洞，该漏洞源于攻击者可以通过imageloadfont强制读取无效内存地址，以触发拒绝服务或获取敏感信息。 |
| 风险影响： | 影响PHP:7.4.0版本(含)到7.4.33版本,8.0.0版本(含)到8.0.25版本,8.1.0版本(含)到8.1.12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.php.net/ChangeLog-8.php#8.0.25 |
| 参考资料： | http://www.php.net |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-15323 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP 缓冲区错误漏洞(CVE-2022-31630)【低可信】 |
| 风险等级： | 高 |
| 高可利用： | 否 |
| CVE编号： | CVE-2022-31630 |
| 端口(服务)： | 8081(PHP) |
| 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。】PHP是一种在服务器端执行的脚本语言。 PHP 8.1.12之前版本存在安全漏洞，该漏洞源于攻击者可以通过imageloadfont强制读取无效内存地址，以触发拒绝服务或获取敏感信息。 |
| 风险影响： | 影响PHP:7.4.0版本(含)到7.4.33版本,8.0.0版本(含)到8.0.25版本,8.1.0版本(含)到8.1.12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.php.net/ChangeLog-8.php#8.0.25 |
| 参考资料： | http://www.php.net |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-15323 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx SSL会话固定漏洞(CVE-2014-3616)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2014-3616 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx　0.5.6－1.7.4版本在实现上存在会话固定漏洞，攻击者可利用此漏洞劫持任意会话或访问敏感信息。<\*来源：Antoine Delignat-Lavaud \*> |
| 风险影响： | 影响nginx:0.5.6版本(含)到1.7.4版本(含) |
| 解决方案： | Nginx-----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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12019 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0747)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0747 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver未正确限制CNAME解析度。通过任意名称解析相关矢量，远程攻击者可造成worker进程资源耗尽，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12021 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 环境问题漏洞(CVE-2020-12440)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2020-12440 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | NGINX是美国NGINX公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。 NGINX中存在环境问题漏洞。攻击者可利用该漏洞进行缓存投毒，劫持凭证或绕过安全保护。 |
| 风险影响： | 影响nginx:1.18.0以下版本(含) |
| 解决方案： | 厂商补丁:https://www.nginx.com/ |
| 参考资料： | https://www.nginx.com/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12944 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 未授权访问漏洞(CVE-2019-20372)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-20372 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | Nginx 1.17.7之前版本中存在未授权访问漏洞。攻击者可利用该漏洞读取未授权的Web页面。 |
| 风险影响： | Nginx<1.17.7 |
| 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://nginx.org/en/CHANGES |
| 参考资料： | https://usn.ubuntu.com/4235-1/ https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2020\_11519&lang=ZH-CN |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-13810 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 中间人攻击漏洞(CVE-2011-4968)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2011-4968 |
| 端口(服务)： | 80(nginx) |
| 风险描述： | NGINX http代理模块中存在安全漏洞。攻击者可利用该漏洞实施中间人攻击。 |
| 风险影响： | 0.7.61≤Nginx≤1.2.6 |
| 解决方案： | 建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://nginx.org/cn/ |
| 参考资料： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201301-039 https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2019\_10556&lang=ZH-CN |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-13876 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx SSL会话固定漏洞(CVE-2014-3616)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2014-3616 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx　0.5.6－1.7.4版本在实现上存在会话固定漏洞，攻击者可利用此漏洞劫持任意会话或访问敏感信息。<\*来源：Antoine Delignat-Lavaud \*> |
| 风险影响： | 影响nginx:0.5.6版本(含)到1.7.4版本(含) |
| 解决方案： | Nginx-----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：http://nginx.org/en/download.html |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12019 |

|  |  |
| --- | --- |
| 漏洞名称 | nginx resolver 拒绝服务漏洞(CVE-2016-0747)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2016-0747 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | nginx是一款使用非常广泛的高性能web服务器。nginx 1.8.1之前版本、1.9.10之前的1.9.x版本中，resolver未正确限制CNAME解析度。通过任意名称解析相关矢量，远程攻击者可造成worker进程资源耗尽，导致拒绝服务。 |
| 风险影响： | 影响nginx:0.6.18版本(含)到1.8.1版本,1.9.0版本(含)到1.9.10版本 |
| 解决方案： | 厂商补丁:Nginx-----Nginx已经为此发布了一个安全公告（049700）以及相应补丁:049700：nginx security advisory (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747)链接：http://mailman.nginx.org/pipermail/nginx/2016-January/049700.html 补丁链接：https://trac.nginx.org/nginx/changeset/93d70d87914c350948ab701cc99569680320e198/nginx |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12021 |

|  |  |
| --- | --- |
| 漏洞名称 | NGINX 环境问题漏洞(CVE-2020-12440)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2020-12440 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | NGINX是美国NGINX公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。 NGINX中存在环境问题漏洞。攻击者可利用该漏洞进行缓存投毒，劫持凭证或绕过安全保护。 |
| 风险影响： | 影响nginx:1.18.0以下版本(含) |
| 解决方案： | 厂商补丁:https://www.nginx.com/ |
| 参考资料： | https://www.nginx.com/ |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-12944 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 未授权访问漏洞(CVE-2019-20372)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2019-20372 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | Nginx 1.17.7之前版本中存在未授权访问漏洞。攻击者可利用该漏洞读取未授权的Web页面。 |
| 风险影响： | Nginx<1.17.7 |
| 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://nginx.org/en/CHANGES |
| 参考资料： | https://usn.ubuntu.com/4235-1/ https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2020\_11519&lang=ZH-CN |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-13810 |

|  |  |
| --- | --- |
| 漏洞名称 | Nginx 中间人攻击漏洞(CVE-2011-4968)【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2011-4968 |
| 端口(服务)： | 8081(nginx) |
| 风险描述： | NGINX http代理模块中存在安全漏洞。攻击者可利用该漏洞实施中间人攻击。 |
| 风险影响： | 0.7.61≤Nginx≤1.2.6 |
| 解决方案： | 建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://nginx.org/cn/ |
| 参考资料： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201301-039 https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2019\_10556&lang=ZH-CN |
| 协议类型： | http |
| 风险举证: | nginx: 0.8.54 |
| 漏洞ID： | SF-0005-13876 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP password\_verify失效认证漏洞通告（CVE-2023-0567）【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-0567 |
| 端口(服务)： | 80(PHP) |
| 风险描述： | PHP（全称：PHP：Hypertext Preprocessor，即“超文本预处理器”）是一种开源的计算机脚本语言，适用于Web开发并可嵌入HTML中，password\_verify() 函数用于验证密码是否和散列值匹配。近日，新华三攻防实验室威胁预警团队监测到PHP官方发布了安全公告，修复了一个存在于password\_verify中的失效认证漏洞（CVE-2023-0567），且漏洞利用代码已公开，攻击者利用该漏洞可导致应用程序允许任何密码都有效。\n影响范围：\n8.1.x <= PHP <8.1.16\n8.2.x <= PHP <8.2.23\n8.0.x <= PHP <8.0.28\n参考链接：https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4 |
| 风险影响： | 影响PHP:8.1.0版本(含)到8.1.16版本,8.2版本(含)到8.2.3版本,8.0版本(含)到8.0.28版本 |
| 解决方案： | 厂商补丁:目前官方已修复该漏洞，受影响用户可以升级更新到安全版本。官方下载链接：https://github.com/php/php-src/tags |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-17018 |

|  |  |
| --- | --- |
| 漏洞名称 | PHP password\_verify失效认证漏洞通告（CVE-2023-0567）【低可信】 |
| 风险等级： | 中 |
| 高可利用： | 否 |
| CVE编号： | CVE-2023-0567 |
| 端口(服务)： | 8081(PHP) |
| 风险描述： | PHP（全称：PHP：Hypertext Preprocessor，即“超文本预处理器”）是一种开源的计算机脚本语言，适用于Web开发并可嵌入HTML中，password\_verify() 函数用于验证密码是否和散列值匹配。近日，新华三攻防实验室威胁预警团队监测到PHP官方发布了安全公告，修复了一个存在于password\_verify中的失效认证漏洞（CVE-2023-0567），且漏洞利用代码已公开，攻击者利用该漏洞可导致应用程序允许任何密码都有效。\n影响范围：\n8.1.x <= PHP <8.1.16\n8.2.x <= PHP <8.2.23\n8.0.x <= PHP <8.0.28\n参考链接：https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4 |
| 风险影响： | 影响PHP:8.1.0版本(含)到8.1.16版本,8.2版本(含)到8.2.3版本,8.0版本(含)到8.0.28版本 |
| 解决方案： | 厂商补丁:目前官方已修复该漏洞，受影响用户可以升级更新到安全版本。官方下载链接：https://github.com/php/php-src/tags |
| 参考资料： |  |
| 协议类型： | http |
| 风险举证: | PHP: 8.1.11 |
| 漏洞ID： | SF-0005-17018 |