# **（1）F5 BIG-IP信息泄露漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP信息泄露漏洞的详情信息。漏洞的编号为：CNVD-2023-75596，CVE编号为：CVE-2023-41253，漏洞威胁等级为：中危，影响产品：F5 BIG-IP (DNS, LTM enabled with DNS Services license3) >=13.1.0，<=13.1.5、F5 BIG-IP (DNS, LTM enabled with DNS Services license3) >=14.1.0，<=14.1.5、F5 BIG-IP (DNS, LTM enabled with DNS Services license3) >=15.1.0，<=15.1.8、F5 BIG-IP (DNS, LTM enabled with DNS Services license3) >=16.1.0，<=16.1.3，漏洞危害：F5 BIG-IP存在信息泄露漏洞，攻击者可利用该漏洞以明文形式查看TSIG密钥。

# **（2）F5 BIG-IP APM信息泄露漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP APM信息泄露漏洞的详情信息。漏洞的编号为：CNVD-2023-75599，CVE编号为：CVE-2023-39447，漏洞威胁等级为：中危，影响产品：F5 BIG-IP (Guided Configuration) 8.0、F5 BIG-IP (Guided Configuration) 6.0、F5 BIG-IP (APM) >=16.1.0，<=16.1.3、F5 BIG-IP (APM) >=15.1.0，<=15.1.7、F5 BIG-IP (Guided Configuration) >=7.0，<=7.7，漏洞危害：F5 BIG-IP APM存在信息泄露漏洞，攻击者可利用该漏洞读取未公开的敏感信息。

# **（3）F5 BIG-IP配置实用程序目录遍历漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP配置实用程序目录遍历漏洞的详情信息。漏洞的编号为：CNVD-2023-75610，CVE编号为：CVE-2023-41373，漏洞威胁等级为：高危，影响产品：F5 BIG-IP (all modules) >=13.1.0，<=13.1.5、F5 BIG-IP (all modules) >=14.1.0，<=14.1.5、F5 BIG-IP (all modules) >=15.1.0，<=15.1.10、F5 BIG-IP (all modules) >=16.1.0，<=16.1.4、F5 BIG-IP (all modules) 17.1.0，漏洞危害：F5 BIG-IP配置实用程序存在目录遍历漏洞，经过身份验证的攻击者可利用该漏洞在BIG-IP系统上执行命令。

# **（4）F5 BIG-IP拒绝服务漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP拒绝服务漏洞的详情信息。漏洞的编号为：CNVD-2023-75597，CVE编号为：CVE-2023-44487，漏洞威胁等级为：中危，影响产品：F5 BIG-IP (all modules) >=13.1.0，<=13.1.5、F5 BIG-IP (all modules) >=14.1.0，<=14.1.5、F5 BIG-IP (all modules) >=15.1.0，<=15.1.10、F5 BIG-IP (all modules) >=16.1.0，<=16.1.4、F5 BIG-IP (all modules) 17.1.0、F5 BIG-IP Next (all modules) 20.0.1、F5 BIG-IP Next SPK >=1.5.0，<=1.8.2、F5 BIG-IP Next CNF >=1.1.0，<=1.1.1、Nginx NGINX Plus >=R25，<=R30、F5 NGINX Open Source >=1.9.5，<=1.25.2、F5 NGINX Ingress Controller >=1.12.2，<=1.12.5、F5 NGINX Ingress Controller >=2.0.0，<=2.4.2、F5 NGINX Ingress Controller >=3.0.0，<=3.3.0，漏洞危害：F5 BIG-IP存在拒绝服务漏洞，攻击者可利用该漏洞导致拒绝服务。

# **（5）F5 BIG-IP信息泄露漏洞、F5 BIG-IP访问控制错误漏洞、F5 BIG-IP会话过期不足漏洞、F5 BIG-IP拒绝服务漏洞、F5 BIG-IP iControl安全绕过漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP信息泄露漏洞、F5 BIG-IP访问控制错误漏洞、F5 BIG-IP会话过期不足漏洞、F5 BIG-IP拒绝服务漏洞、F5 BIG-IP iControl安全绕过漏洞的详情信息。影响产品：F5 BIG-IP (all modules) >=13.1.0，<=13.1.5、F5 BIG-IP (all modules) >=16.1.0，<=16.1.3、F5 BIG-IP (all modules) >=14.1.0，<=14.1.5、F5 BIG-IP (all modules) >=15.1.0，<=15.1.8。其中高危漏洞有5个，漏洞编号为：CNVD-2023-75601（CVE-2023-43746）、CNVD-2023-75602（CVE-2023-40537）、CNVD-2023-75604（CVE-2023-40542）、CNVD-2023-75606（CVE-2023-41085）、CNVD-2023-75609（CVE-2023-42768），中危漏洞有1个，漏洞编号为：CNVD-2023-75598（CVE-2023-45219），漏洞危害：F5 BIG-IP存在信息泄露漏洞，攻击者可利用该漏洞查看敏感信息。F5 BIG-IP存在访问控制错误漏洞，攻击者可利用该漏洞越过安全边界。F5 BIG-IP存在会话过期不足漏洞，攻击者可利用该漏洞在有限的时间内重用由Configuration实用程序生成的身份验证用户的会话cookie，并通过管理端口和/或自IP地址进行访问，以执行任意系统命令、创建或删除文件或禁用服务。F5 BIG-IP存在拒绝服务漏洞，攻击者可利用该漏洞导致内存资源利用率的增加。F5 BIG-IP存在拒绝服务漏洞，攻击者可利用该漏洞导致流量管理微内核(TMM)终止。F5 BIG-IP iControl存在安全绕过漏洞，攻击者可利用该漏洞是BIP-IP非管理员用户仍然可以访问iControl REST管理员资源。

# **（6）F5 BIG-IP信息泄露漏洞、F5 BIG-IP敏感信息明文存储漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP信息泄露漏洞、F5 BIG-IP敏感信息明文存储漏洞的详情信息。影响产品：F5 BIG-IP (all modules) >=13.1.0，<=13.1.5、F5 BIG-IP (all modules) >=16.1.0，<=16.1.3、F5 BIG-IP (all modules) >=14.1.0，<=14.1.5、F5 BIG-IP (all modules) >=15.1.0，<=15.1.8、F5 BIG-IQ Centralized Management >=8.0.0，<=8.3.0。其中中危漏洞有2个，漏洞编号为：CNVD-2023-75595（CVE-2023-43485）、CNVD-2023-75600（CVE-2023-41964），漏洞危害：F5 BIG-IP存在信息泄露漏洞，攻击者可利用该漏洞查看共享密钥。F5 BIG-IP存在敏感信息明文存储漏洞，攻击者可利用该漏洞获取对特权信息的访问权。

# **（7）F5 BIG-IP HTTP/2服务拒绝漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP HTTP/2服务拒绝漏洞的详情信息。漏洞的编号为：CNVD-2023-75605，CVE编号为：CVE-2023-40534，漏洞威胁等级为：高危，影响产品：F5 BIG-IP (all modules) >=16.1.0，<=16.1.4、F5 BIG-IP (all modules) 17.1.0、F5 BIG-IP Next SPK >=1.6.0，<=1.8.2，漏洞危害：F5 BIG-IP HTTP/2存在服务拒绝漏洞，攻击者可利用该漏洞导致TMM终止。

# **（8）F5 BIG-IP Edge客户端加密签名验证错误漏洞、F5 BIG-IP Edge数据验证错误漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP Edge客户端加密签名验证错误漏洞、F5 BIG-IP Edge数据验证错误漏洞的详情信息。影响产品：F5 BIG-IP Edge客户端 >=7.2.3，<=7.2.4。其中中危漏洞有2个，漏洞编号为：CNVD-2023-75603（CVE-2023-43611）、CNVD-2023-75608（CVE-2023-5450），漏洞危害：F5 BIG-IP Edge客户端存在加密签名验证错误漏洞，攻击者可利用该漏洞滥用正在进行的边缘客户端安装，以获取客户端macOS系统上的本地特权升级。F5 BIG-IP Edge存在数据验证错误漏洞，攻击者可利用该漏洞在安装过程中提升权限。

# **（9）F5 BIG-IP Next SPK硬编码凭证漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于F5 BIG-IP Next SPK硬编码凭证漏洞的详情信息。漏洞的编号为：CNVD-2023-75607，CVE编号为：CVE-2023-45226，漏洞威胁等级为：高危，影响产品：F5 BIG-IP Next SPK 1.5.0，漏洞危害：F5 BIG-IP Next SPK存在硬编码凭证漏洞，具有拦截流量能力的攻击者可利用该漏洞在这些容器上冒充SPK Secure Shell (SSH)服务器。

# **（10）Google Android拒绝服务漏洞、Google Android权限提升漏洞、Google Android代码执行漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于Google Android拒绝服务漏洞、Google Android权限提升漏洞、Google Android代码执行漏洞的详情信息。影响产品：Google Android 11.0、Google Android 12.0、Google Android 13.0、Google Android 12.1。其中高危漏洞有4个，漏洞编号为：CNVD-2023-75540（CVE-2023-35667）、CNVD-2023-75542（CVE-2023-35673）、CNVD-2023-75543（CVE-2023-35665）、CNVD-2023-75544（CVE-2023-35684），中危漏洞有1个，漏洞编号为：CNVD-2023-75538（CVE-2023-35677），漏洞危害：Google Android存在拒绝服务漏洞，攻击者可利用此漏洞导致拒绝服务。Google Android存在权限提升漏洞，攻击者可利用此漏洞在系统上获得提升的权限。Google Android存在代码执行漏洞，攻击者可利用此漏洞在系统上运行任意代码。Google Android存在权限提升漏洞，攻击者可利用此漏洞升级权限。

# **（11）Google Android权限提升漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于Google Android权限提升漏洞的详情信息。影响产品：Google Android 11.0、Google Android 12.1、Google Android 12.0、Google Android 13.0。其中高危漏洞有2个，漏洞编号为：CNVD-2023-75539（CVE-2023-35666）、CNVD-2023-75541（CVE-2023-35687），漏洞危害：Google Android存在权限提升漏洞，攻击者可利用此漏洞导致权限提升。Google Android存在权限提升漏洞，攻击者可利用此漏洞在系统上获得提升的权限。

# **（12）Google Android权限提升漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Google Android权限提升漏洞的详情信息。影响产品：Google Android 12.0、Google Android 13.0、Google Android 12.1、Google android 11.0。其中高危漏洞有2个，漏洞编号为：CNVD-2023-75536（CVE-2023-35669）、CNVD-2023-75537（CVE-2023-35670），漏洞危害：Google Android存在权限提升漏洞，攻击者可利用此漏洞在系统上获得提升的权限。

# **（13）Google Chrome安全绕过漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Google Chrome安全绕过漏洞的详情信息。漏洞的编号为：CNVD-2023-75504，CVE编号为：CVE-2022-3660，漏洞威胁等级为：中危，影响产品：Google Chrome <107.0.5304.62，漏洞危害：Google Chrome存在安全漏洞，该漏洞源于在全屏模式下执行不当。攻击者可利用此漏洞绕过安全限制。

# **（14）Google Chrome安全绕过漏洞、Google Chrome安全绕绕过漏洞**

2023年10月10日、2023年10月09日，国家信息安全漏洞共享平台（CNVD）公开关于Google Chrome安全绕过漏洞、Google Chrome安全绕绕过漏洞的详情信息。影响产品：Google Chrome <117.0.5938.62。其中中危漏洞有10个，漏洞编号为：CNVD-2023-75496（CVE-2023-4900）、CNVD-2023-75497（CVE-2023-4903）、CNVD-2023-75498（CVE-2023-4902）、CNVD-2023-75499（CVE-2023-4907）、CNVD-2023-75500（CVE-2023-4906）、CNVD-2023-75501（CVE-2023-4909）、CNVD-2023-75502（CVE-2023-4901）、CNVD-2023-75503（CVE-2023-4905）、CNVD-2023-75321（CVE-2023-4904）、CNVD-2023-75320（CVE-2023-4908），漏洞危害：Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Custom Tabs模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Custom Mobile Tabs模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Input模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Intents模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome存在安全绕过漏洞，该漏洞源于Autofill模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Interstitials模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome存在安全绕过漏洞，该漏洞源于Prompts模块的不当实现。攻击者可利用该漏洞绕过安全限制。Google Chrome存在安全绕过漏洞，该漏洞源于Downloads模块策略执行不充分。攻击者可利用该漏洞绕过安全限制。Google Chrome 117.0.5938.62之前版本存在安全绕过漏洞，该漏洞源于Picture模块的不当实现。攻击者利用该漏洞绕过安全限制。

# **（15）Microsoft 3D Builder远程代码执行漏洞**

2023年10月09日，国家信息安全漏洞共享平台（CNVD）公开关于Microsoft 3D Builder远程代码执行漏洞的详情信息。影响产品：Microsoft 3D Builder。其中高危漏洞有4个，漏洞编号为：CNVD-2023-74907（CVE-2023-36773）、CNVD-2023-74908（CVE-2023-36772）、CNVD-2023-74909（CVE-2023-36771）、CNVD-2023-74910（CVE-2023-36770），漏洞危害：Microsoft 3D Builder存在远程代码执行漏洞，攻击者可利用该漏洞在系统上执行任意代码。

# **（16）Microsoft 3D Viewer远程代码执行漏洞**

2023年10月09日，国家信息安全漏洞共享平台（CNVD）公开关于Microsoft 3D Viewer远程代码执行漏洞的详情信息。影响产品：Microsoft 3D Viewer <7.2307.27042.0。其中高危漏洞有3个，漏洞编号为：CNVD-2023-74904（CVE-2023-36740）、CNVD-2023-74905（CVE-2023-36739）、CNVD-2023-74906（CVE-2023-36760），漏洞危害：Microsoft 3D Viewer存在远程代码执行漏洞，攻击者可利用该漏洞在目标主机上执行代码。

# **（17）Microsoft Azure HDInsight Apache Ambari权限提升漏洞**

2023年10月09日，国家信息安全漏洞共享平台（CNVD）公开关于Microsoft Azure HDInsight Apache Ambari权限提升漏洞的详情信息。漏洞的编号为：CNVD-2023-74911，CVE编号为：CVE-2023-38156，漏洞威胁等级为：高危，影响产品：Microsoft Azure HDInsights，漏洞危害：Microsoft Azure HDInsight Apache Ambari存在权限提升漏洞，攻击者可利用该漏洞获取域管理员权限。

# **（18）Mozilla Firefox远程代码执行漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox远程代码执行漏洞的详情信息。漏洞的编号为：CNVD-2023-75350，CVE编号为：CVE-2022-34483，漏洞威胁等级为：高危，影响产品：Mozilla Firefox <102.0，漏洞危害：Mozilla Firefox存在远程代码执行漏洞，该漏洞源于拖放图像功能缺少对于扩展名的限制与过滤。攻击者可利用该漏洞通过拖放恶意图像到文件系统执行恶意代码。

# **（19）Mozilla Thunderbird和Firefox拒绝服务漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Thunderbird和Firefox拒绝服务漏洞的详情信息。漏洞的编号为：CNVD-2023-75347，CVE编号为：CVE-2022-46881，漏洞威胁等级为：高危，影响产品：Mozilla Firefox <106.0、Mozilla Firefox ESR <102.6、Mozilla Thunderbird <102.6，漏洞危害：Mozilla Thunderbird、Firefox和Firefox ESR的WebGL存在拒绝服务漏洞。攻击者可利用该漏洞破坏内存并导致程序崩溃。

# **（20）Mozilla Firefox内存破坏漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox内存破坏漏洞的详情信息。漏洞的编号为：CNVD-2023-75349，CVE编号为：CVE-2022-46878，漏洞威胁等级为：高危，影响产品：Mozilla Firefox <108.0、Mozilla Firefox ESR <102.6、Mozilla Thunderbird <102.6，漏洞危害：Mozilla Firefox存在内存破坏漏洞，远程攻击者可利用该漏洞提交特殊的web请求，诱使用户解析，可使应用程序崩溃或者可以应用程序上下文执行任意代码。

# **（21）Mozilla Firefox代码问题漏洞、Mozilla Firefox ESR内存破坏代码执行漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox代码问题漏洞、Mozilla Firefox ESR内存破坏代码执行漏洞的详情信息。影响产品：Mozilla Firefox <117.0、Mozilla Firefox ESR <102.15、Mozilla Firefox ESR >=115.0，<115.2、Mozilla Thunderbird <115.2。其中高危漏洞有2个，漏洞编号为：CNVD-2023-75344（CVE-2023-4573）、CNVD-2023-75345（CVE-2023-4584），漏洞危害：Mozilla Firefox存在代码问题漏洞，该漏洞源于当通过IPC接收渲染数据时，mStream初始化时可能会被破坏，攻击者可利用该漏洞导致释放后使用，从而导致潜在的可利用崩溃。Mozilla Firefox ESR存在内存破坏漏洞，远程攻击者可利用该漏洞提交特殊的WEB请求，诱使用户解析，可使应用程序崩溃或以应用程序上下文执行任意代码。

# **（22）Mozilla Firefox内存错误引用漏洞、Mozilla Firefox ImageBitmap存在释放后使用漏洞**

2023年10月10日、2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox内存错误引用漏洞、Mozilla Firefox ImageBitmap存在释放后使用漏洞的详情信息。影响产品：Mozilla Firefox <118。其中高危漏洞有2个，漏洞编号为：CNVD-2023-75343（CVE-2023-5172）、CNVD-2023-75342（CVE-2023-5175），漏洞危害：Mozilla Firefox内存错误引用漏洞，远程攻击者可以利用该漏洞提交特殊的Web请求，诱使用户解析，可使应用程序崩溃。Mozilla Firefox ImageBitmap在进程关闭时存在释放后使用漏洞，远程攻击者可以利用该漏洞提交特殊的Web请求，诱使用户解析，可使应用程序崩溃。

# **（23）Mozilla Firefox资源操作不当漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox资源操作不当漏洞的详情信息。漏洞的编号为：CNVD-2023-75348，CVE编号为：CVE-2022-22755，漏洞威胁等级为：高危，影响产品：Mozilla Firefox <97.0，漏洞危害：Mozilla Firefox存在资源操作不当漏洞，该漏洞源于浏览器处理XSL文档的方式。攻击者可利用该漏洞欺骗受害者加载一个特别设计的XSL文档，该文档可以在同源策略的范围内继续执行JavaScript，即使在浏览器选项卡关闭之后。

# **（24）Mozilla Firefox ESR代码问题漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox ESR代码问题漏洞的详情信息。漏洞的编号为：CNVD-2023-75346，CVE编号为：CVE-2023-29548，漏洞威胁等级为：高危，影响产品：Mozilla Firefox ESR <102.10、Mozilla Thunderbird <102.10、mozilla Firefox Android <112.0、Mozilla firefox focus <112.0、Mozilla focus android <112.0，漏洞危害：Mozilla Firefox ESR存在代码问题漏洞，该漏洞源于Ion编译器中存在错误的降低指令，攻击者可利用该漏洞导致ARM64上的优化结果不正确。

# **（25）Mozilla Firefox整数溢出漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于Mozilla Firefox整数溢出漏洞的详情信息。漏洞的编号为：CNVD-2023-75351，CVE编号为：CVE-2022-34481，漏洞威胁等级为：高危，影响产品：Mozilla Thunderbird <91.11、Mozilla Firefox ESR <91.11、Mozilla Firefox <102.0，漏洞危害：Mozilla Firefox存在整数溢出漏洞，该漏洞源于应用中的nsTArray\_Impl::ReplaceElementsAt()函数中对于输入的数据存在不当的验证，攻击者可利用该漏洞通过使用对于容器太大的替换元素时，可能会发生整数溢出。

# **（26）NXLog Manager跨站请求伪造漏洞**

2023年10月07日，国家信息安全漏洞共享平台（CNVD）公开关于NXLog Manager跨站请求伪造漏洞的详情信息。漏洞的编号为：CNVD-2023-74533，CVE编号为：CVE-2023-32792，漏洞威胁等级为：高危，影响产品：Nxlog nxlog manager 5.6.5633，漏洞危害：NXLog Manager存在跨站请求伪造漏洞，远程攻击者可以利用该漏洞提交特殊的恶意请求，可以目标用户上下文执行恶意操作。

# **（27）Online Pizza Ordering System SQL注入漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Online Pizza Ordering System SQL注入漏洞的详情信息。漏洞的编号为：CNVD-2023-76374，CVE编号为：CVE-2023-5423，漏洞威胁等级为：中危，影响产品：Online Pizza Ordering System Online Pizza Ordering System 1.0，漏洞危害：Online Pizza Ordering System存在SQL注入漏洞，攻击者可利用该漏洞通过脚本查看、添加、修改或删除后端数据库中的信息。

# **（28）Open5GS访问控制错误漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Open5GS访问控制错误漏洞的详情信息。漏洞的编号为：CNVD-2023-76460，CVE编号为：CVE-2023-4884，漏洞威胁等级为：高危，影响产品：Open5GS Open5GS <=2.4.10，漏洞危害：Open5GS 2.4.10及之前版本存在访问控制错误漏洞，该漏洞源于缺乏身份验证，攻击者可利用该漏洞向Open5GS端点发送HTTP请求，并检索存储在设备上的信息。

# **（29）PortlandLabs Concrete CMS SEO-Extra功能跨站脚本漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于PortlandLabs Concrete CMS SEO-Extra功能跨站脚本漏洞的详情信息。漏洞的编号为：CNVD-2023-76459，CVE编号为：CVE-2023-44766，漏洞威胁等级为：中危，影响产品：PortlandLabs Concrete CMS v9.2.1，漏洞危害：PortlandLabs Concrete CMS SEO-Extra功能存在跨站脚本漏洞，攻击者可利用该漏洞通过页面设置中SEO-Extra的特制脚本执行任意代码。

# **（30）Siemens SICAM PAS/PQS权限分配不正确漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SICAM PAS/PQS权限分配不正确漏洞的详情信息。漏洞的编号为：CNVD-2023-75593，CVE编号为：CVE-2023-45205，漏洞威胁等级为：高危，影响产品：SIEMENS SICAM PAS/PQS >= V8.00，< V8.20，漏洞危害：Siemens SICAM PAS/PQS存在权限分配不正确漏洞，攻击者可利用该漏洞注入任意代码并将权限提升到NT AUTHORITY/SYSTEM。

# **（31）Siemens SICAM PAS/PQS权限分配不正确漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SICAM PAS/PQS权限分配不正确漏洞的详情信息。漏洞的编号为：CNVD-2023-75594，CVE编号为：CVE-2023-38640，漏洞威胁等级为：中危，影响产品：SIEMENS SICAM PAS/PQS >= V8.00，< V8.22，漏洞危害：Siemens SICAM PAS/PQS存在权限分配不正确漏洞，攻击者可利用该漏洞在应用程序进程的上下文中读取和修改配置数据。

# **（32）Siemens SICAM A8000设备CPCI85固件硬编码凭据漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SICAM A8000设备CPCI85固件硬编码凭据漏洞的详情信息。漏洞的编号为：CNVD-2023-75592，CVE编号为：CVE-2023-36380，漏洞威胁等级为：高危，影响产品：Siemens CP-8031 MASTER MODULE (6MF2803-1AA00) < CPCI85 V05.11 (only with activated debug support)、Siemens CP-8050 MASTER MODULE (6MF2805-0AA00) < CPCI85 V05.11 (only with activated debug support)，漏洞危害：Siemens SICAM A8000设备CPCI85固件存在硬编码凭据漏洞，攻击者可利用该漏洞通过SSH登录到设备。只有具有已激活调试支持的设备才会受到影响。

# **（33）Siemens SICAM A8000设备CPCI85固件Web服务器路径遍历漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SICAM A8000设备CPCI85固件Web服务器路径遍历漏洞的详情信息。漏洞的编号为：CNVD-2023-75577，CVE编号为：CVE-2023-42796，漏洞威胁等级为：高危，影响产品：Siemens CP-8031 MASTER MODULE (6MF2803-1AA00) < CPCI85 V05.11、Siemens CP-8050 MASTER MODULE (6MF2805-0AA00) < CPCI85 V05.11，漏洞危害：Siemens SICAM A8000设备CPCI85固件Web服务器存在路径遍历漏洞，攻击者可利用该漏洞遍历系统上的目录并下载任意文件。通过探查活动会话ID，将权限提升到管理员角色。

# **（34）Siemens Mendix Forgot Password模块户枚举漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens Mendix Forgot Password模块户枚举漏洞的详情信息。漏洞的编号为：CNVD-2023-75589，CVE编号为：CVE-2023-43623，漏洞威胁等级为：中危，影响产品：Siemens Mendix Forgot Password (Mendix 7 compatible) < V3.7.3、Siemens Mendix Forgot Password (Mendix 8 compatible) < V4.1.3、Siemens Mendix Forgot Password (Mendix 9 compatible) < V5.4.0、Siemens Mendix Forgot Password (Mendix 10 compatible) < V5.4.0，漏洞危害：Siemens Mendix Forgot Password模块存在户枚举漏洞，攻击者可利用该漏洞能够确定用户是否有效，从而对有效用户进行暴力攻击。

# **（35）Siemens Parasolid堆栈缓冲区溢出漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens Parasolid堆栈缓冲区溢出漏洞的详情信息。漏洞的编号为：CNVD-2023-75579，CVE编号为：CVE-2023-45601，漏洞威胁等级为：高危，影响产品：Siemens Parasolid V35.0 < V35.0.262、Siemens Parasolid V35.1 < V35.1.250、Siemens Parasolid V36.0 < V36.0.169，漏洞危害：Siemens Parasolid存在堆栈缓冲区溢出漏洞，该漏洞是由于受影响的应用程序在分析精心编制的IGS文件时包含堆栈溢出漏洞。攻击者可利用该漏洞在当前进程的上下文中执行代码。

# **（36）Siemens SIMATIC CP设备资源消耗失控漏洞、Siemens SIMATIC CP设备访问控制不当漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SIMATIC CP设备资源消耗失控漏洞、Siemens SIMATIC CP设备访问控制不当漏洞的详情信息。影响产品：Siemens SIMATIC CP 1604 (6GK1160-4AA01)、Siemens SIMATIC CP 1616 (6GK1161-6AA02)、Siemens SIMATIC CP 1623 (6GK1162-3AA00)、Siemens SIMATIC CP 1626 (6GK1162-6AA01)、Siemens SIMATIC CP 1628 (6GK1162-8AA00)。其中中危漏洞有2个，漏洞编号为：CNVD-2023-75575（CVE-2023-37195）、CNVD-2023-75576（CVE-2023-37194），漏洞危害：Siemens SIMATIC CP设备存在资源消耗失控漏洞，该漏洞是由于受影响的设备无法充分控制直接内存访问（DMA）请求的连续映射。攻击者可利用该漏洞在主机上造成拒绝服务。需要物理电源循环才能使系统重新工作。Siemens SIMATIC CP设备存在访问控制不当漏洞，该漏洞是由于受影响设备的内核内存通过直接内存访问（DMA）暴露在用户模式下，攻击者可利用该漏洞在主机系统上无任何限制地执行任意代码。

# **（37）Siemens SINEC NMS跨站脚本漏洞、Siemens SINEC NMS权限分配不正确漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SINEC NMS跨站脚本漏洞、Siemens SINEC NMS权限分配不正确漏洞的详情信息。影响产品：Siemens SINEC NMS < V2.0。其中高危漏洞有1个，漏洞编号为：CNVD-2023-75591（CVE-2022-30527），中危漏洞有1个，漏洞编号为：CNVD-2023-75590（CVE-2023-44315），漏洞危害：Siemens SINEC NMS存在跨站脚本漏洞，该漏洞是由于受影响的应用程序不正确地清除从受监控设备检索到的某些SNMP配置数据。攻击者可利用该漏洞导致合法用户无意中修改应用程序数据。Siemens SINEC NMS存在权限分配不正确漏洞，该漏洞是由于受影响的应用程序为包含可执行文件和库的特定文件夹分配了不正确的访问权限。攻击者可利用该漏洞注入任意代码并提升权限。

# **（38）Siemens SINEMA Server V14跨站脚本漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens SINEMA Server V14跨站脚本漏洞的详情信息。漏洞的编号为：CNVD-2023-75578，CVE编号为：CVE-2023-35796，漏洞威胁等级为：高危，影响产品：Siemens SINEMA Server V14，漏洞危害：Siemens SINEMA Server V14存在跨站脚本漏洞，该漏洞是由于受影响的应用程序不正确地清除从受监控设备检索到的某些SNMP配置数据。攻击者可利用该漏洞在应用程序服务器上使用SYSTEM权限执行任意代码。

# **（39）Siemens Simcenter Amesim远程代码执行漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens Simcenter Amesim远程代码执行漏洞的详情信息。漏洞的编号为：CNVD-2023-75588，CVE编号为：CVE-2023-43625，漏洞威胁等级为：高危，影响产品：Siemens Simcenter Amesim < V2021.1，漏洞危害：Siemens Simcenter Amesim存在远程代码执行漏洞，攻击者可利用该漏洞在受影响应用程序进程的上下文中执行DLL注入和执行任意代码。

# **（40）Siemens Tecnomatix Plant Simulation越界读取漏洞、Siemens Tecnomatix Plant Simulation越界写入漏洞、Siemens Tecnomatix Plant Simulation文件分析漏洞**

2023年10月13日、2023年10月12日、2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens Tecnomatix Plant Simulation越界读取漏洞、Siemens Tecnomatix Plant Simulation越界写入漏洞、Siemens Tecnomatix Plant Simulation文件分析漏洞的详情信息。影响产品：Siemens Tecnomatix Plant Simulation V2201 < V2201.0009、Siemens Tecnomatix Plant Simulation V2302 < V2302.0003。其中高危漏洞有8个，漏洞编号为：CNVD-2023-75581（CVE-2023-44087）、CNVD-2023-75582（CVE-2023-44086）、CNVD-2023-75583（CVE-2023-44085）、CNVD-2023-75584（CVE-2023-44084）、CNVD-2023-75585（CVE-2023-44083）、CNVD-2023-75586（CVE-2023-44082）、CNVD-2023-75587（CVE-2023-44081）、CNVD-2023-75580（CVE-2023-45204），漏洞危害：Siemens Tecnomatix Plant Simulation存在越界读取漏洞，由于在解析特制的SPP文件时，受影响的应用程序包含超过分配结构末尾的越界读取。攻击者可利用该漏洞在当前进程的上下文中执行代码。Siemens Tecnomatix Plant Simulation存在越界写入漏洞，由于在解析特制的SPP文件时，受影响的应用程序包含超过已分配缓冲区末尾的越界写入。攻击者可利用该漏洞在当前进程的上下文中执行代码。Siemens Tecnomatix Plant Simulation存在文件分析漏洞，该漏洞是由于受影响的应用程序在分析精心编制的IGS文件时包含类型混淆漏洞。攻击者可利用该漏洞在当前进程的上下文中执行代码。

# **（41）Siemens Xpedition Layout Browser堆栈溢出漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于Siemens Xpedition Layout Browser堆栈溢出漏洞的详情信息。漏洞的编号为：CNVD-2023-75574，CVE编号为：CVE-2023-30900，漏洞威胁等级为：高危，影响产品：Siemens Xpedition Layout Browser < VX.2.14，漏洞危害：Siemens Xpedition Layout Browser存在堆栈溢出漏洞，攻击者可利用该漏洞在当前进程的上下文中执行代码。

# **（42）TOTOLINK A3002R缓冲区溢出漏洞**

2023年10月13日，国家信息安全漏洞共享平台（CNVD）公开关于TOTOLINK A3002R缓冲区溢出漏洞的详情信息。漏洞的编号为：CNVD-2023-76373，CVE编号为：CVE-2022-40112，漏洞威胁等级为：高危，影响产品：TOTOLINK A3002R V1.1.1-B20200824.0128，漏洞危害：TOTOLINK A3002R存在缓冲区溢出漏洞，攻击者可利用该漏洞导致拒绝服务。

# **（43）WordPress Ezoic存在跨站脚本漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress Ezoic存在跨站脚本漏洞的详情信息。漏洞的编号为：CNVD-2023-74808，CVE编号为：CVE-2022-41132，漏洞威胁等级为：中危，影响产品：WordPress Ezoic <=2.8.8，漏洞危害：WordPress Ezoic2.8.8及之前版本存在跨站脚本漏洞，该漏洞源于对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞窃取受害者基于cookie的身份验证凭据。

# **（44）WordPress Log HTTP Requests跨站脚本漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress Log HTTP Requests跨站脚本漏洞的详情信息。漏洞的编号为：CNVD-2023-74813，CVE编号为：CVE-2022-3402，漏洞威胁等级为：中危，影响产品：WordPress Log HTTP Requests <=1.3.1，漏洞危害：WordPress Log HTTP Requests plugin 1.3.1及其之前版本存在跨站脚本漏洞，攻击者可利用该漏洞窃取受害者基于cookie的身份验证凭据。

# **（45）WordPress Permalink Manager Lite跨站请求伪造漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress Permalink Manager Lite跨站请求伪造漏洞的详情信息。漏洞的编号为：CNVD-2023-74811，CVE编号为：CVE-2022-4021，漏洞威胁等级为：高危，影响产品：WordPress Permalink Manager Lite <=2.2.20.1，漏洞危害：WordPress Permalink Manager Lite 2.2.20.1及其之前版本存在跨站请求伪造漏洞，该漏洞源于在extra\_actions函数上缺少或不正确的nonce验证，攻击者可利用漏洞进行跨站点脚本攻击、Web缓存中毒和其他恶意活动。

# **（46）WordPress ProfileGrid CSV注入漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress ProfileGrid CSV注入漏洞的详情信息。漏洞的编号为：CNVD-2023-74809，CVE编号为：CVE-2022-41791，漏洞威胁等级为：中危，影响产品：WordPress ProfileGrid <=5.1.6，漏洞危害：WordPress ProfileGrid5.1.6及之前版本存在CSV注入漏洞，攻击者可利用该漏洞发起更改授权攻击。

# **（47）WordPress Quiz And Survey Master SQL注入漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress Quiz And Survey Master SQL注入漏洞的详情信息。漏洞的编号为：CNVD-2023-74814，CVE编号为：CVE-2021-36898，漏洞威胁等级为：高危，影响产品：WordPress Quiz And Survey Master <=7.3.4，漏洞危害：WordPress Quiz And Survey Master plugin 7.3.4及其之前版本存在SQL注入漏洞，该漏洞源于应用缺少对外部输入SQL语句的验证。攻击者可利用该漏洞执行非法SQL命令窃取数据库数据。

# **（48）WordPress插件WPML Multilingual CMS premium访问控制错误漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress插件WPML Multilingual CMS premium访问控制错误漏洞的详情信息。漏洞的编号为：CNVD-2023-74810，CVE编号为：CVE-2022-38461，漏洞威胁等级为：中危，影响产品：WordPress WPML Multilingual CMS premium <=4.5.10，漏洞危害：WordPress插件WPML Multilingual CMS premium存在访问控制错误漏洞，该漏洞源于应用存在不当的访问控制，攻击者可利用漏洞更改插件设置。

# **（49）WordPress Web Stories plugin输入验证错误漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress Web Stories plugin输入验证错误漏洞的详情信息。漏洞的编号为：CNVD-2023-74817，CVE编号为：CVE-2022-3708，漏洞威胁等级为：高危，影响产品：WordPress Web Stories <1.25.0，漏洞危害：WordPress Web Stories plugin 1.25.0之前版本存在输入验证错误漏洞，该漏洞源于其/v1/hotlink/proxy REST API端点的url参数对URL验证不足，攻击者可利用漏洞可以向来自web应用程序的任意位置发出web请求，并可用于查询和修改来自内部服务的信息。

# **（50）WordPress demon image annotation跨站请求伪造漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress demon image annotation跨站请求伪造漏洞的详情信息。漏洞的编号为：CNVD-2023-74812，CVE编号为：CVE-2022-2864，漏洞威胁等级为：高危，影响产品：WordPress demon image annotation <=4.7，漏洞危害：WordPress demon image annotation 4.7及其之前版本存在跨站请求伪造漏洞，该漏洞源于其~/includes/settings.php文件中缺少nonce验证，攻击者可利用漏洞修改插件的设置并通过伪造的请求注入恶意Web脚本。

# **（51）WordPress theme Bricks授权问题漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress theme Bricks授权问题漏洞的详情信息。漏洞的编号为：CNVD-2023-74815，CVE编号为：CVE-2022-3400，漏洞威胁等级为：高危，影响产品：WordPress theme Bricks >=1.0，<=1.5.3，漏洞危害：WordPress theme Bricks plugin 1.0及其之后，1.5.3及其之前版本存在授权问题漏洞，该漏洞源于其缺少对bricks\_save\_post AJAX操作的功能检查，攻击者可利用漏洞编辑易受攻击的WordPress网站上的任何页面、帖子或模板。

# **（52）WordPress theme Bricks远程代码执行漏洞**

2023年10月08日，国家信息安全漏洞共享平台（CNVD）公开关于WordPress theme Bricks远程代码执行漏洞的详情信息。漏洞的编号为：CNVD-2023-74816，CVE编号为：CVE-2022-3401，漏洞威胁等级为：高危，影响产品：WordPress theme Bricks >=1.2，<1.5.4，漏洞危害：WordPress theme Bricks plugin 1.2及其之后，1.5.4之前版本存在远程代码执行漏洞。攻击者可利用漏洞编辑易受攻击的WordPress网站上的任何页面、帖子或模板，并注入可用于实现远程代码执行的代码执行块。

# **（53）cURL SOCKS5堆溢出漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于cURL SOCKS5堆溢出漏洞的详情信息。漏洞的编号为：CNVD-2023-75809，CVE编号为：CVE-2023-38545，漏洞威胁等级为：高危，影响产品：cURL libcurl >=7.69.0，<=8.3.0，漏洞危害：cURL SOCKS5存在堆溢出漏洞，攻击者可利用该漏洞构造恶意主机名，造成代码执行。

# **（54）任子行下一代防火墙存在信息泄露漏洞**

2023年10月10日，国家信息安全漏洞共享平台（CNVD）公开关于任子行下一代防火墙存在信息泄露漏洞的详情信息。漏洞的编号为：CNVD-2023-71385，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：低危，影响产品：任子行网络技术股份有限公司 任子行下一代防火墙 V10.0，漏洞危害：任子行下一代防火墙存在信息泄露漏洞，攻击者可利用该漏洞获取敏感信息。

# **（55）启明星辰天玥网络安全审计系统存在命令执行漏洞**

2023年10月12日、2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于启明星辰天玥网络安全审计系统存在命令执行漏洞的详情信息。影响产品：启明星辰信息技术集团股份有限公司 天玥网络安全审计系统 IBM-N2080#V6.0。其中高危漏洞有2个，漏洞编号为：CNVD-2023-71706（该漏洞无CVE编号）、CNVD-2023-71712（无对应CVE编号），漏洞危害：启明星辰天玥网络安全审计系统存在命令执行漏洞，攻击者可利用该漏洞获取服务器权限。

# **（56）浙江大华技术股份有限公司智慧园区综合管理平台存在SQL注入漏洞**

2023年10月11日，国家信息安全漏洞共享平台（CNVD）公开关于浙江大华技术股份有限公司智慧园区综合管理平台存在SQL注入漏洞的详情信息。漏洞的编号为：CNVD-2023-71714，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：高危，影响产品：浙江大华技术股份有限公司 智慧园区综合管理平台，漏洞危害：浙江大华技术股份有限公司智慧园区综合管理平台存在SQL注入漏洞，攻击者可以利用漏洞获取数据库配置信息。

# **（57）QQ音乐存在命令执行漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于QQ音乐存在命令执行漏洞的详情信息。漏洞的编号为：CNVD-2023-71686，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：高危，影响产品：深圳市腾讯计算机系统有限公司 QQ音乐，漏洞危害：QQ音乐存在命令执行漏洞，攻击者可利用该漏洞执行任意命令。

# **（58）珠海金山办公软件有限公司WPS Windows版存在命令执行漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于珠海金山办公软件有限公司WPS Windows版存在命令执行漏洞的详情信息。漏洞的编号为：CNVD-2023-71685，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：高危，影响产品：珠海金山办公软件有限公司 WPS Windows版 <=12.1.0.15336，漏洞危害：珠海金山办公软件有限公司WPS Windows版存在命令执行漏洞，攻击者可利用该漏洞执行任意代码。

# **（59）用友网络科技股份有限公司NC Cloud存在远程命令执行漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于用友网络科技股份有限公司NC Cloud存在远程命令执行漏洞的详情信息。漏洞的编号为：CNVD-2023-71023，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：高危，影响产品：用友网络科技股份有限公司 NC Cloud，漏洞危害：用友网络科技股份有限公司NC Cloud存在远程命令执行漏洞，攻击者可利用漏洞通过构造恶意请求绕过校验进行远程命令执行，从而获取服务器权限。

# **（60）科大讯飞股份有限公司API网关管理系统存在信息泄露漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于科大讯飞股份有限公司API网关管理系统存在信息泄露漏洞的详情信息。漏洞的编号为：CNVD-2022-43434，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：中危，影响产品：科大讯飞股份有限公司 API网关管理系统 V3.3.0、科大讯飞股份有限公司 API网关管理系统 V3.5.1，漏洞危害：科大讯飞股份有限公司API网关管理系统存在信息泄露漏洞，攻击者可利用该漏洞获取敏感信息。

# **（61）Pouch存在容器逃逸漏洞**

2023年10月12日，国家信息安全漏洞共享平台（CNVD）公开关于Pouch存在容器逃逸漏洞的详情信息。漏洞的编号为：CNVD-2023-71698，CVE编号为：该漏洞无CVE编号，漏洞威胁等级为：低危，影响产品：阿里云计算有限公司 Pouch <=1.3.1，漏洞危害：Pouch存在容器逃逸漏洞，攻击者可利用该漏洞在容器的宿主机文件系统上写任意文件。