2023-08-08

0day&1day&重点 Nday 漏洞预警

目录

【0day】某远 OA 远程代码执行漏洞预警

基本情况

某远 OA A8 是一款流行的协同管理软件，在各中、大型企业机构中广泛使用。

近日监测发现 某远 OA 存在远程代码执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 某远 OA V8.0
- 某远 OA V7.1、V7.1SP1
- 某远 OA V7.0、V7.0SP1、V7.0SP2、V7.0SP3
- 其他未确认版本需自查

处置建议

通用修复建议：

目前某远 OA 官方未发布安全版本或补丁修复这些漏洞，建议受影响用户针对以下路径进行访问策略限制。

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager

实际利用路径有以下多种：

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&requestCompress=gzip

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&requestCompress=gzip&managerMethod=checkDB&arguments=**payload**

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&managerMethod=checkDB&arguments=**payload**

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfigManager&managerMethod=**存在多个参数均受影响**&arguments=**payload**

参考链接

1) https://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=1

【0day】华某 OA 远程代码执行漏洞预警

基本情况

华某软件有限公司是国内首批专注于独立 OA 协同软件研发、为政企提供垂直专业、数智化转型解决方案的科技创新型企业。自 200

1 年成立以来，华某动力服务网络覆盖全国，并依托智慧协同平台、工作流引擎及智能报表引擎三大核心技术，深耕前瞻科技与政企业务场景的深入融合，充分赋能政企数智化转型及精益智慧管理建设进程的推进和完善。。

近日监测发现 华某 OA 存在远程代码执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查，当前情报为最新版本受影响

处置建议

通用修复建议：

目前华某 OA 官方未发布安全版本或补丁修复这些漏洞，建议受影响用户针对以下路径进行访问策略限制。

/OAapp/bfapp/*

实际利用有以下多种特征：

getClass()、eval、java.lang.Thread.currentThread()

参考链接

暂无

【0day】36x 终端安全管理审计系统存在漏洞预警

基本情况

36x 终端安全管理系统是在 36x 全网数字安全大脑极致赋能下，以云计算、大数据、人工智能等新技术为支撑，以可靠服务为保障，集防病毒、漏洞修复、终端合规管控、终端准入、终端审计、数据防泄漏管理于一体的企业级安全产品，能同时兼容传统与信创终端统一管理、全面保障政企终端安全。。

近日监测发现 36x 终端安全管理系统存在漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查

处置建议

通用修复建议：

暂无

参考链接

暂无

【0day】某凌 oa 远程代码执行漏洞预警

基本情况

某凌 oa 是一款流行的协同管理软件，在各中、大型企业机构中广泛使用。

近日监测发现 某凌 oa 存在远程代码执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 某凌 oa V15 及以下版本
- 其他未确认版本需自查

处置建议

通用修复建议：

目前某凌 oa 官方未发布安全版本或补丁修复这些漏洞，建议受影响用户针对以下路径进行访问策略限制。

/api///sys/ui/sys_ui_extend/sysUiExtend.do

实际利用路径有以下多种：

/api///*

参考链接

暂无

【0day】某达 OA 后台远程代码执行漏洞预警

基本情况

某达 OA 是一款流行的协同管理软件，在各中、大型企业机构中广泛使用。

近日监测发现某达 OA 后台存在远程代码执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 某达 OA V11.10 及以前版本
- 其他未确认版本需自查

处置建议

通用修复建议：

目前某达 OA 官方未发布安全版本或补丁修复这些漏洞，建议受影响用户针对以下路径进行访问策略限制。

/module/upload/upload.php

参考链接

暂无

【0day】亿某通电子文档安全管理系统任意文件上传漏洞预警

基本情况

亿某通电子文档安全管理系统（简称：CDG）是一款电子文档安全加密软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产，对电子文档进行全生命周期防护，系统具有透明加密、主动加密、智能加密等多种加密方式，用户可根据部门涉密程度的不同（如核心部门和普通部门），部署力度轻重不一的梯度式文档加密防护，实现技术、管理、审计进行有机的结合，在内部构建起立体化的整体信息防泄露体系，使得成本、效率和安全三者达到平衡，实现电子文档的数据安全。

近日监测发现亿某通电子文档安全管理系统任意文件上传漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 其他未确认版本需自查

处置建议

通用修复建议：

目前亿某通官方未发布安全版本或补丁修复这些漏洞，建议受影响用户针对以下路径进行访问策略限制。

/CDGServer3/UploadFileFromClientServiceForClient

/CDGServer3/UsersService

参考链接

暂无

【1day】某盟堡垒机任意用户密码读取漏洞预警

基本情况

近日监测发现某盟堡垒机存在任意用户密码读取漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上获取任意用户密码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查

处置建议

通用修复建议：

官方已给出修复补丁包，建议升级更新。以下为关键路径：

/webservice/soapclient.php

参考链接

暂无

【1day】某盟堡垒机任意命令执行漏洞预警

基本情况

近日监测发现某盟堡垒机存在任意命令执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意命令。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查

处置建议

通用修复建议：

官方已给出修复补丁包，建议升级更新。以下为关键路径：

/api/virtual/*

参考链接

暂无

【1day】某恒堡垒机任意命令执行漏洞预警

基本情况

近日监测发现某恒堡垒机存在任意命令执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意命令。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查

处置建议

通用修复建议：

官方已给出修复补丁包，建议升级更新。以下为关键路径：

/webapi/dbaudit/*

参考链接

暂无

【1day】某恒 EDR 任意命令执行漏洞预警

基本情况

近日监测发现某恒 EDR 存在任意命令执行漏洞，攻击者可通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任意命令。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- 未确认版本需自查

处置建议

通用修复建议：

官方已给出修复补丁包，建议升级更新。以下为关键路径：

/service/api/admin/user/*

参考链接

暂无

【Nday】Apache Log4j2 远程代码执行漏洞

基本情况

Apache Log4j2 是一个开源的 Java 日志框架，被广泛地应用在中间件、开发 框架与 Web 应用中。

由于 Apache Log4j2 某些功能存在递归解析功能，攻击者可直接构造恶意请求，触发远程代码执行漏洞。漏洞利用无需特殊配置，经 36x 漏洞云验证，Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等均受影响。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- Apache Log4j<2.15.0-rc1

处置建议

通用修复建议：

1、排查应用是否引入了 Apache log4j-core Jar 包，若存在依赖引入，且在受影响版本范围内，则可能存在漏洞影响。同时为了避免在 Apache Log4j 2.15.0 版本中某些自定义配置而可能导致的 JNDI 注入或拒绝服务攻击，请尽快升级 Apache Log4j2 所有相关应用到 2.16.0 或者 2.12.2 及其以上版本，地址 https://logging.apache.org/log4j/2.x/download.html 。

2、对于 Java 8 及其以上用户，建议升级 Apache Log4j2 至 2.16.0 及以上版本。

3、对于 Java 7 用户，建议升级至 Apache Log4j 2.12.2 及以上版本，该版本为安全版本，用于解决兼容性问题。

4、对于其余暂时无法升级版本的用户，建议删除 JndiLookup，可用以下命令 zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

5、升级已知受影响的应用及组件，如 spring-boot-starter/log4j2/Apache Struts2/Apache Solr/Apache Druid/Apache Flink

【Nday】VMware vCenter Server 远程代码执行漏洞预警

基本情况

VMware vCenter Server 是 VMware 虚拟化管理平台，广泛的应用于企业私有云内网中。通过使用 vCenter，管理员可以轻松的管理上百台虚拟化环境 。

vSphere Client（HTML5） 在 vCenter Server 插件中存在一个远程执行代码漏洞。未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，写入 webshell，控制服务器。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- VMware vCenterServer<=7.0 U1c
- VMware vCenterServer<=6.7 U31
- VMware vCenterServer<=6.5 U3n
- VMware Cloud Foundation=4.2
- VMware Cloud Foundation=3.10.1.2

处置建议

通用修复建议：

官方已发布新版本中修复上述漏洞，受影响用户请尽快升级到安全版本。

VMware:vCenter Server:

7.0 版本升级到 7.0 U2b 下载链接：

https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u2b-release-notes.html

6.7 版本升级到 6.7 U3n 下载链接：

https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3n-release-notes.html

6.5 版本升级到 6.5 U3p 下载链接：

https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3p-release-notes.html

VMware:Cloud Foundation:

4.x 版本升级到 4.2.1 下载链接：

https://docs.vmware.com/en/VMware-Cloud-Foundation/4.2.1/rn/VMware-Cloud-Foundation-421-Release-Notes.html

3.x 版本升级到 3.10.2.1 下载链接：

https://docs.vmware.com/en/VMware-Cloud-34Foundation/3.10.2/rn/VMware-Cloud-Foundation-3102-Release-Notes.html#3.10.2.1

参考链接

1）https://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=1

【Nday】Apache Shiro 存在身份验证绕过漏洞预警

基本情况

Apache Shiro 是一个开源安全框架，提供身份验证、授权、密码学和会话管理。Shiro 框架直观、易用，同时也能提供健壮的安全性。

Apache Shiro 在 1.12.0 或 2.0.0-alpha-3 之前与基于非规范化请求路由的 API 和 Web 框架一起使用时，可能会受到路径遍历攻击，导致身份验证绕过。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

影响范围

- Apache Shiro < 1.12.0
- Apache Shiro < 2.0.0-alp

处置建议

通用修复建议：

厂商已发布了漏洞修复程序，请使用此产品的用户尽快更新至安全版本：

Apache Shiro 1.12.0

Apache Shiro 2.0.0-alpha-3

官方下载链接：https://shiro.apache.org/blog/2023/07/18/apache-shiro-1120-released.html

参考链接

暂无