2023HW 必修高危漏洞集合

版本：v2.0

2023.07

斗象科技 – 漏洞情报中信

Email: service@tophant.com

Tel: 400-156-9866

目录

一、 前言

高危风险漏洞一直是企业网络安全防护的薄弱点，也成为 HW 攻防演练期间红队的重要突破口；每年 HW 期间爆发了大量的高危风险漏洞成为红队突破网络边界防护的一把利器，很多企业因为这些高危漏洞而导致整个防御体系被突破、甚至靶标失守而遗憾出局。

HW 攻防演练在即，斗象情报中心依托漏洞盒子的海量漏洞数据、情报星球社区的一手漏洞情报资源以及 Freebuf 安全门户的安全咨询进行分析整合，输出 HW 必修高危漏洞手册，意在帮助企业在 HW 攻防演练的前期进行自我风险排查，降低因高危漏洞而“城池失守”的风险。

本次报告整合了近两年在攻防演练被红队利用最频繁且对企业危害较高的漏洞，包含了详细的漏洞基础信息、检测规则和修复方案，企业可根据自身资产信息进行针对性的排查、配置封堵策略和漏洞修复相关工作。

斗象智能安全 PRS 已支持详细检测规则，如需要协助请联系：400-156-9866

HW 必修高危漏洞集合持续更新中，请持续关注。

二、 漏洞汇总数据

本文档对 22 年以前危害较高且利用率较高的漏洞进行了总结，同时对近期爆发的高危漏洞进行补充，22-23 年高危必修漏洞可参考已经发布的《HW 必修高危漏洞集合_v1.0》文档，具体的数据如下所示：

- 命令执行

  漏洞数量：6 个

  涉及厂商：Apache、Apache HTTPd、H3C、HIKVISION、Spring Cloud

- 远程代码执行

  漏洞数量：3 个

  涉及厂商：Atlassian、Metabase

- 文件上传

  漏洞数量：4 个

  涉及厂商：FineReport、大华、海康威视

- 其他

  漏洞类型包含：SQL 注入、反序列化、任意文件读取等

以下为本次高危漏洞自查列表：

漏洞名称	漏洞类型	所属厂商	影响版本
Apache RocketMQ 远程代码执行漏洞 (CVE-2023-37582)	命令执行	Apache	5.0.0 <= version <= 5.1.1 4.0.0 <= version <= 4.9.6
泛微 e-cology9 XXE 漏洞	XXE	泛微	泛微 e-cology9 协同办公系统 < 10.58.1
Weblogic 远程代码执行漏洞 (CVE-2023-21931)	远程代码执行	Oracle	WebLogic Server 12.2.1.3.0 WebLogic Server 12.2.1.4.0 WebLogic Server

			14.1.1.0.0
海康威视 iSecure Center 综合安防 文件上传漏洞	文件上传	海康威视	海康威视 综合安防
金蝶云星空软件 远程代码执行漏洞	反序列化	金蝶云	金蝶云星空 V8.X 金蝶云星空 V7.X 金蝶云星空 <= V6.2 及以下所有私有云版本
瑞友天翼应用虚拟化系统 远程代码执行漏洞	SQL 注入	瑞友	5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1
Fortinet FortiOS SSL-VPN 远程代码执行漏洞 (CVE-2023-27997)	缓冲区溢出	Fortinet	Fortinet FortiOS < 7.2.5 Fortinet FortiOS < 7.0.12 Fortinet FortiOS < 6.4.13 Fortinet FortiOS < 6.2.15 Fortinet FortiOS < 6.0.1712
用友 NC Cloud 任意文件写入漏洞	文件写入	用友	用友 NC Cloud
大华智慧园区综合管理平台 文件上传漏洞 (CVE-2023-3836)	文件上传	大华	大华智慧园区综合管理平台
大华智慧园区综合管理平台 远程代码执行	文件上传	大华	大华智慧园区综合管理平台 <=

漏洞			V3.001.0000004.18.R.2223994
Apache Shiro存在身份验证绕过漏洞 (CVE-2023-34478)	逻辑漏洞	Apache	Apache Shiro < 1.12.0 Apache Shiro < 2.0.0-alpha-3
Metabase 远程代码执行漏洞 (CVE-2023-38646)	远程代码执行	Metabase	Metabase < 0.46.6.1 Metabase Enterprise Edition < 1.46.6.1 Metabase < 0.45.4.1 Metabase Enterprise Edition < 1.45.4.1 Metabase < 0.44.7.1 Metabase Enterprise Edition < 1.44.7.1 Metabase < 0.43.7.2 Metabase Enterprise Edition < 1.43.7.2
HIKVISION DS/IDS/IPC 等设备 远程命令执行漏洞 (CVE-2021-36260)	命令执行	HIKVISION	详见漏洞详情
Spring Cloud Gateway 远程命令执行漏洞 (CVE-2022-22947)	命令执行	Spring Cloud	Spring Cloud Gateway <= 3.1.0 3.0.0 <= Spring Cloud Gateway <= 3.0.6 Spring Cloud Gateway 旧的、不受支持的版本也受影响
Zabbix 未授权访问	未授权访	Zabbix	5.4.0 <= Zabbixx <=

(CVE-2022-23131)	问		5.4.8 Zabbixx 6.0.0alpha1
Apache HTTPd 命令执行漏洞 (CVE-2021-41773)	命令执行	Apache HTTPd	Apache HTTP Server 2.4.49 Apache HTTP Server 2.4.50
Apache HTTPd 命令执行漏洞 (CVE-2021-42013)	命令执行	Apache HTTPd	Apache HTTP Server 2.4.49 Apache HTTP Server 2.4.50
Atlassian Jira cfx 任意文件读取漏洞 (CVE-2021-26086)	任意文件读取	Atlassian Jira	Atlassian Jira Server and Data Center < 8.5.14 8.6.0 ≤ Atlassian Jira Server and Data Center < 8.13.6 8.14.0 ≤ Atlassian Jira Server and Data Center < 8.16.1
Apache Druid 远程代码执行漏洞 (CVE-2021-25646)	远程代码执行	Apache Druid	Apache Druid < 0.20.1
Django SQL 注入漏洞 (CVE-2021-35042)	SQL 注入	Django	Django 3.2 Django 3.1
Grafana 文件读取漏洞 (CVE-2021-43798)	任意文件读取	Grafana	8.0.0-beta1 <= Grafana <= 8.3.0
FineReport 文件上传漏洞	文件上传	FineReport	FineReport 9.0

(CNVD-2021-34467)			
H3C Intelligent Management Center 命令执行漏洞 (CNVD-2021-39067)	命令执行	H3C	H3C Intelligent Management Center

三、 自查高危详情

3.1 Apache RocketMQ 远程代码执行漏洞 (CVE-2023-37582)

1) 漏洞描述

Apache RocketMQ 是一个分布式消息中间件，它支持多种消息模式，如发布/订阅、点对点、广播等，以及多种消息类型，如有序消息、延迟消息、批量消息等。它具有高吞吐量、低延迟、高可靠性、高可扩展性等特点，适用于互联网、大数据、移动互联网、物联网等领域的实时数据处理。

RocketMQ NameServer 组件仍然存在远程命令执行漏洞，CVE-2023-33246 问题在 5.1.1 版本中尚未完全修复。

2) 披露时间

2023 年 7 月 12 日

3) 影响版本

5.0.0 <= Apache RocketMQ <= 5.1.1

4.0.0 <= Apache RocketMQ <= 4.9.6

4) 检测规则

查看 RocketMQ 中的 Nameserver 的 namesrv.log 日志文件中更新配置参数是否存在恶意命令

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

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 RocketMQ 5.1.2

Apache RocketMQ 4.9.7

官方下载地址：https://rocketmq.apache.org/zh/download

3.2 泛微 e-cology9 XXE 漏洞

1) 漏洞描述

泛微协同管理应用平台（e-cology）是一套兼具企业信息门户、知识管理、数据中心、工作流管理、人力资源管理、客户与合作伙伴管理、项目管理、财务管理、资产管理功能的协同商务平台。

泛微 e-cology9 协同办公系统在 10.58.1 补丁之前存在 XXE 漏洞。未经授权的攻击者可利用该漏洞列目录、读取文件，甚至可能获取应用系统的管理员权限。

2) 爆发时间

2023 年 7 月 13 日

3) 影响版本

泛微 e-cology9 协同办公系统 < 10.58.1

4) 检测规则

查看流量设备中的 URL 是否存在 /rest/ofs/deleteUserRequestInfoByXml 的相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复程序，建议用户升级到如下版本：

泛微 e-cology9 协同办公系统 10.58.1

官方下载地址：https://www.weaver.com.cn/cs/securityDownload.html

3.3 Weblogic 远程代码执行漏洞(CVE-2023-21931)

1) 漏洞描述

WebLogic 是美商 Oracle 的主要产品之一，系购并得来。是商业市场上主要的 Java 应用服务器软件之一，是世界上第一个成功商业化的 J2EE 应用服务器，目前已推出到 14c 版。

WebLogic 存在远程代码执行漏洞，未经授权的攻击者利用此漏洞构造恶意请求发送给 WebLogic 服务器，成功利用此漏洞后攻击者可以接管 WebLogic 服务器，并执行任意命令。

2) 爆发时间

2023 年 4 月 18 日

3) 影响版本

WebLogic Server 12.2.1.3.0

WebLogic Server 12.2.1.4.0

WebLogic Server 14.1.1.0.0

4) 检测规则

查看流量设备中是否存在关键字: 00424541080103000000000。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复补丁，下载链接：https://www.oracle.com/security-alerts/cpuapr2023.html

3.4 海康威视 iSecure Center 综合安防 文件上传漏洞

1) 漏洞描述

iSecure Center 综合安防管理平台是一套“集成化”、“智能化”的平台，通过接入视频监控、一卡通、停车场、报警检测等系统的设备，获取边缘节点数据，实现安防信息化集成与联动。

iSecure Center 综合安防管理平台存在文件上传漏洞。未经授权的攻击者可以上传恶意 Webshell 文件，从而进一步控制服务器。

2) 爆发时间

2023 年 6 月 20 日

3) 影响版本

海康威视 iSecure Center 综合安防

4) 检测规则

查看流量设备中的 URL 是否存在 /center/api/files; 的相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

下载地址：https://open.hikvision.com/download/5c67f1e2f05948198c909700?type=10

3.5 金蝶云星空软件 远程代码执行漏洞

1) 漏洞描述

金蝶云星空是一款基于云计算、大数据、社交、人工智能、物联网等前沿技术研发的新一代战略性企业管理软件。

金蝶云星空的多个版本存在反序列化漏洞。未经身份认证的攻击者可以利用该漏洞执行任意代码，导致服务器被控制。

2) 爆发时间

2023 年 6 月 15 日

3) 影响版本

金蝶云星空 V8.X

金蝶云星空 V7.X

金蝶云星空 <= V6.2 及以下所有私有云版本

4) 检测规则

查看流量设备中 URL 中是否存在 /K3Cloud/Kingdees.BOS.ServiceFacade.ServicesStub.BusinessData.BusinessDataService.Audit.common.kdsvc 相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

官方下载地址：https://vip.kingdee.com/knowledge/specialDetail/352491453127123200?category=352491970117034240&id=388994085535220992&productLineId=1。

3.6 瑞友天翼应用虚拟化系统 远程代码执行漏洞

1) 漏洞描述

瑞友天翼应用虚拟化系统是一种基于服务器计算架构的应用虚拟化平台，可以将各种应用软件集中部署在服务器上，客户端通过 WEB 访问授权的应用软件，实现远程接入和协同办公。

瑞友天翼应用虚拟化系统在 5.x 至 7.0.2.1 版本中存在远程代码执行漏洞。未授权的攻击者可以利用该漏洞来执行任意命令，写入后门，从而入侵服务器，获取服务器权限，直接导致服务器沦陷。

2) 爆发时间

2023 年 4 月 10 日

3) 影响版本

5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1

4) 检测规则

查看流量设备中是否存在对 /AgentBoard.XGI 路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复程序，建议用户升级到如下版本：

瑞友天翼应用虚拟化系统 > 7.0.2.1

官方下载地址：http://www.realor.cn/product/xiazaishiyong/

3.7 Fortinet FortiOS SSL-VPN 远程代码执行漏洞 (CVE-2023-27997)

1) 漏洞描述

Fortinet FortiOS SSL-VPN 是一款安全的虚拟专用网络（VPN）解决方案，可以让远程用户通过 SSL 加密的 HTTPS 链接访问企业内部的网络资源。

Fortinet FortiOS 在多个版本中存在远程代码执行漏洞。这是一个堆溢出漏洞，可以通过 HTTPS 链接触发。它可能让未经认证的远程攻击者在设备上执行任意代码。

2) 爆发时间

2023 年 6 月 12 日

3) 影响版本

Fortinet FortiOS < 7.2.5

Fortinet FortiOS < 7.0.12

Fortinet FortiOS < 6.4.13

Fortinet FortiOS < 6.2.15

Fortinet FortiOS < 6.0.1712

4) 检测规则

查看流量设备中是否存在对 /remote/info 路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本。

3.8 用友 NC Cloud 任意文件写入漏洞

1) 漏洞描述

用友 NC Cloud 大型企业数字化平台，深度应用新一代数字智能技术，完全基于云原生架构，打造开放、互联、融合、智能的一体化云平台。

用友 NC Cloud 中存在任意文件写入漏洞。未经授权的攻击者可以利用该漏洞写入恶意的 Webshell 文件，进而控制服务器。

2) 爆发时间

2023 年 3 月 16 日

3) 影响版本

NC Cloud1909

NC Cloud2020.05

NC Cloud2021.05

NC Cloud2021.11

4) 检测规则

查看流量中是否存在 /uapjs/jsinvoke/?action=invoke 相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

官方下载地址：https://www.yonyou.com.sg/zh/products/nc-cloud/

3.9 大华智慧园区综合管理平台 文件上传漏洞 (CVE-2023-3836)

1) 漏洞描述

大华智慧园区综合管理平台是一个基于智能物联技术的园区安防、办公、运营的数字化解决方案。

大华智慧园区综合管理平台(截至 20230713)版本中存在文件上传漏洞。未经授权的攻击者可以上传恶意 Webshell 的 JSP 文件，可以进行 RCE 利用。

2) 爆发时间

2023 年 7 月 22 日

3) 影响版本

大华智慧园区综合管理平台 <= 20230713 之前发行版本

4) 检测规则

查看流量中是否存在 /emap/devicePoint_addImgIco?hasSubsystem=true 相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

官方咨询地址：https://support.dahuatech.com/afterSales

3.10 大华智慧园区综合管理平台 远程代码执行漏洞

1) 漏洞描述

大华智慧园区综合管理平台是一个基于智能物联技术的园区安防、办公、运营的数字化解决方案。

大华智慧园区综合管理平台在 V3.001.0000004.18.R.2223994 及之前版本中存在远程代码执行漏洞。未经授权的攻击者可以上传恶意 Webshell 的 JSP 文件，可以进行 RCE 利用。

2) 爆发时间

2023 年 5 月 29 日

3) 影响版本

大华智慧园区综合管理平台 <= V3.001.0000004.18.R.2223994

4) 检测规则

检查流量中是否有对 /admin/sso_initSession.action、/admin/user_save.action、/admin/recover_recover.action 路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本。

官方咨询地址：https://support.dahuatech.com/afterSales

3.11 Apache Shiro 存在身份验证绕过漏洞 (CVE-2023-34478)

1) 漏洞描述

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。

2) 爆发时间

2023 年 7 月 24 日

3) 影响版本

Apache Shiro < 1.12.0

Apache Shiro < 2.0.0-alpha-3

4) 检测规则

检查 Apache Shiro 是否有与基于非规范化请求路由一起使用的情况。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

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

3.12 Metabase 远程代码执行漏洞(CVE-2023-38646)

1) 漏洞描述

Metabase 是一款开源的业务智能（BI）工具，可以帮助你把数据库中的数据以可视化的方式呈现给更多人，让他们自己探索数据并发现洞察。

Metabase 在 多个版本中存在远程代码执行漏洞。未经授权的攻击者可以在服务器上执行任意指令，进而控制服务器。

2) 爆发时间

2023 年 7 月 21 日

3) 影响版本

Metabase < 0.46.6.1

Metabase Enterprise Edition < 1.46.6.1

Metabase < 0.45.4.1

Metabase Enterprise Edition < 1.45.4.1

Metabase < 0.44.7.1

Metabase Enterprise Edition < 1.44.7.1

Metabase < 0.43.7.2

Metabase Enterprise Edition < 1.43.7.2

4) 检测规则

检查流量中是否有对 /api/session/properties 路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

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：

Metabase >= 0.46.6.1

Metabase Enterprise Edition >= 1.46.6.1

Metabase >= 0.45.4.1

Metabase Enterprise Edition >= 1.45.4.1

Metabase >= 0.44.7.1

Metabase Enterprise Edition >= 1.44.7.1

Metabase >= 0.43.7.2

Metabase Enterprise Edition >= 1.43.7.2

官方下载链接：https://github.com/metabase/metabase/releases

3.13 HIKVISION DS/IDS/IPC 等设备 远程命令执行漏洞(CVE-2021-36260)

1) 漏洞描述

海康威视部分产品中的 web 模块存在一个命令注入漏洞，由于对输入参数校验不充分，攻击者可以发送带有恶意命令的报文到受影响设备，成功利用此漏洞可以导致命令执行。

2) 爆发时间

2023 年 8 月 4 日

3) 影响版本

序号	产品名称	受影响版本号	修复程序下载
1	DS-2CVxxxx	版本 build 日期在 210625 之前	点击下载
2	DS-2CD1xxx		点击下载
3	IPCxx		点击下载
4	DS-IPC-Bxx DS-IPC-Txx		点击下载
5	DS-IPC-Exx DS-IPC-Sxx DS-IPC-Axx DS-2XDxxxx		点击下载
6	DS-2CD2xxx		点击下载
7	DS-2CD3xxx		点击下载
8	(i)DS-2DCxxxx		点击下载
9	(i)DS-2DExxxx		点击下载

10	(i)DS-2PTxxxx		点击下载
11	(i)DS-2SE7xxxx		点击下载
12	DS-2DBxxxx		点击下载
13	DS-2DYHxxxx		点击下载
14	DS-2DY9xxxx		点击下载
15	iDS-2DY5Cxxx		点击下载
16	iDS-2DP9Cxxx-T4		点击下载
17	DS-2DY7xxx-CX(S5) DS-2DF6xxx-CX(S6) DS-2DF6Cxxx-CX(T2)		点击下载
18	iDS-2VY4xxxx		点击下载
19	iDS-EGDxxxx		点击下载
20	DS-2CD4xxx DS-2CD5xxx		点击下载
21	DS-2CD6xxx		点击下载
22	DS-2CD7xxx DS-GPZxxx		点击下载
23	DS-2CD8xxx		点击下载
24	DS-2XA8xxx		点击下载
25	DS-FCNxxxx		点击下载
26	iDS-2XM/CD6xxx		点击下载
27	DS-2DF5xxxx DS-2DF6xxxx DS-2DF6xxxx-Cx DS-2DF7xxxx DS-2DF8xxxx DS-2DF9xxxx		点击下载

28	iDS-2VPDxxxx iDS-2DPxxxx		点击下载
29	iDS-2PT9xxxx		点击下载
30	iDS-2SK7xxxx iDS-2SK8xxxx		点击下载
31	iDS-2SR8xxxx		点击下载
32	iDS-2VSxxxx		点击下载
33	iDS-2VTxxxx		点击下载
34	iDS-GPZ2xxxx		点击下载
35	DS-2XE62x7FWD(D) DS-2XE30x6FWD(B) DS-2XE60x6FWD(B) DS-2XE62x2F(D) DS-2XC66x5G0 DS-2XE64x2F(B)		点击下载
36	KBA18(C)-83x6FWD		点击下载
37	DS-2TBxxx DS-Bxxxx DS-2TDxxxxB TBC-12xxx TBC-26xxx	版本 build 日期在 210702 之前	点击下载
38	DS-2TD1xxx-xx DS-2TD2xxx-xx		点击下载
39	DS-2TD51xx-xx/W/GLT DS-2TD55xx-xx/W DS-2TD65xx-xx/W		点击下载
40	DS-2TD41xx-xx/Wxx DS-2TD62xx-xx/Wxx		点击下载

	DS-2TD81xx-xx/Wxx DS-2TD91xx-xx/W DS-2TD4xxx-xx/V2 DS-2TD55xx-xx/V2 DS-2TD6xxx-xx/V2 DS-2TD81xx-xx/V2 DS-2TD91xx-xx/V2		
41	DS-76xxN-Exx DS-78xxN-Kxx DS-NVR-K1xx DS-NVR-K2xx	V4.30.210 Build20122 4- V4.31.000 Build210511	点击下载

4) 检测规则

查看流量设备中的 URL 是否存在 /SDK/webLanguage 且请求方法为 PUT 的相关流量。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复补丁，请使用此产品的用户尽快更新安全补丁：

参考链接：https://www.hikvision.com/cn/support/CybersecurityCenter/SecurityNotices/20210919/

3.14 Spring Cloud Gateway 远程命令执行漏洞 (CVE-2022-22947)

1) 漏洞描述

Spring Cloud Gateway 是提供了一个用于在 Spring WebFlux 之上构建 API 网关的库。

Spring Cloud Gateway 存在代码注入漏洞，该漏洞源于当网关执行器端点被启用、暴露和不安全时，应用程序很容易受到代码注入攻击。

远程攻击者可利用该漏洞可以发出恶意的请求，允许在远程主机上执行任意远程命令。

2) 爆发时间

2022 年 3 月 1 日

3) 影响版本

Spring Cloud Gateway <= 3.1.0

3.0.0 <= Spring Cloud Gateway <= 3.0.6

Spring Cloud Gateway 旧的、不受支持的版本也受影响

4) 检测规则

查看流量设备中是否存在相关路由：/actuator/gateway/routes。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

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：

Spring Cloud Gateway >= 3.1.1

Spring Cloud Gateway >= 3.1.7

参考链接：https://start.spring.io/

3.15 Zabbix 未授权访问(CVE-2022-23131)

1) 漏洞描述

Zabbix 是拉脱维亚 Zabbix 公司的一套开源的监控系统。该系统支持网络监控、服务器监控、云监控和应用监控等。

Zabbix 存在安全漏洞，该漏洞源于在启用 SAML SSO 身份验证（非默认）的情况下，恶意行为者可以修改会话数据，因为存储在会话中的用户登录未经过验证。

未经身份验证的恶意攻击者可能会利用此问题来提升权限并获得对 Zabbix 前端的管理员访问权限。

2) 爆发时间

2022 年 1 月 13 日

3) 影响版本

5.4.0 <= Zabbixx <= 5.4.8

Zabbixx 6.0.0alpha1

4) 检测规则

检查是否配置 saml sso 登录。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Zabbixx 5.4.9rc2

Zabbixx 6.0.0beta1

Zabbixx 6.0 (plan)

官方下载链接：https://www.zabbix.com/download

3.16 Apache HTTPd 命令执行漏洞(CVE-2021-41773)

1) 漏洞描述

Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器软件，可以在大多数电脑操作系统中运行。由于其跨平台和安全性，被广泛使用，是最流行的 Web 服务器软件之一。它快速、可靠并且可通过简单的 API 扩展，将 Perl／Python 等解释器编译到服务器中。

在 Apache HTTP Server 2.4.49 中的路径规范化更改中发现了一个漏洞。攻击者可以利用路径遍历攻击将 URL 映射到由 Alias 类似指令配置之外的目录中的文件。如果这些目录之外的文件没有受到通常的默认配置 "require all denied" 的保护，则这些请求可以成功。如果对这些别名路径启用了 CGI 脚本，那么这可能导致远程代码执行。

2) 爆发时间

2021 年 10 月 5 日

3) 影响版本

Apache HTTP Server 2.4.49

Apache HTTP Server 2.4.50

4) 检测规则

查看流量设备中 URL 中是否存在 /cgi-bin/.%2e/.%2e/.%2e/.%2e 或 /icons/.%2e/%2e%2e/%2e%2e/%2e%2e 相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Apache HTTP Server 2.4.51

官方下载链接：https://httpd.apache.org/download.cgi

3.17 Apache HTTPd 命令执行漏洞(CVE-2021-42013)

1) 漏洞描述

Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器软件，可以在大多数电脑操作系统中运行。由于其跨平台和安全性，被广泛使用，是最流行的 Web 服务器软件之一。它快速、可靠并且可通过简单的 API 扩展，将 Perl／Python 等解释器编译到服务器中。

Apache HTTP Server 2.4.50 中对 CVE-2021-41773 的修复不够充分。攻击者可以使用路径遍历攻击将 URL 映射到由类似别名的指令配置的目录之外的文件。如果这些目录之外的文件不受通常的默认配置 “require all denied” 的保护，则这些请求可能会成功。如果还为这些别名路径启用了 CGI 脚本，则可以允许远程代码执行。

2) 爆发时间

2021 年 10 月 5 日

3) 影响版本

Apache HTTP Server 2.4.49

Apache HTTP Server 2.4.50

4) 检测规则

查看流量设备中 URL 中是否存在 /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65 或 /icons/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65 相关字样。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Apache HTTP Server 2.4.51

官方下载链接：https://httpd.apache.org/download.cgi

3.18 Atlassian Jira cfx 任意文件读取漏洞 (CVE-2021-26086)

1) 漏洞描述

Atlassian Jira 是 Atlassian 开发的专有问题跟踪产品，它允许 bug 跟踪和敏捷项目管理。

受影响的 Atlassian Jira Server 和 Data Center 版本允许远程攻击者通过路径遍历漏洞读取特定文件。

2) 爆发时间

2021 年 8 月 15 日

3) 影响版本

Atlassian Jira Server and Data Center < 8.5.14

8.6.0 ≤ Atlassian Jira Server and Data Center < 8.13.6

8.14.0 ≤ Atlassian Jira Server and Data Center < 8.16.1

4) 检测规则

查看流量设备中是否存在对 /s/cfx/_/; 相关路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Atlassian Jira Server and Data Center 8.5.14

Atlassian Jira Server and Data Center 8.13.6

Atlassian Jira Server and Data Center 8.16.1

Atlassian Jira Server and Data Center 8.17.0

官方下载链接：https://www.atlassian.com/software/jira/update

3.19 Apache Druid 远程代码执行漏洞 (CVE-2021-25646)

1) 漏洞描述

Apache Druid 是美国阿帕奇软件（Apache）基金会的一款使用 Java 语言编写的、面向列的开源分布式数据库。

Apache Druid 默认情况下缺乏授权认证，攻击者可以发送特制请求，利用 Druid 服务器上进程的特权执行任意代码。

2) 爆发时间

2021 年 1 月 29 日

3) 影响版本

Apache Druid < 0.20.1

4) 检测规则

查看流量设备中是否存在对 /druid/indexer/v1/sampler 相关路由的请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Apache Druid >= 0.20.1

下载地址：https://druid.apache.org/downloads.html

3.20 Django SQL 注入漏洞(CVE-2021-35042)

1) 漏洞描述

Django 是一个开放源代码的 Web 应用框架，由 Python 写成。采用了 MTV 的软件设计模式，即模型，视图和模板。

Django 组件存在 SQL 注入漏洞，该漏洞是由于对 QuerySet.order_by()中用户提供数据的过滤不足，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行 SQL 注入攻击，最终造成服务器敏感信息泄露。

2) 爆发时间

2021 年 7 月 2 日

3) 影响版本

Django 3.2

Django 3.1

4) 检测规则

查看流量中是否存在 SQL 注入相关语句。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Django >= 3.2.5

Django >= 3.1.13

下载地址：https://www.djangoproject.com/download/

3.21 Grafana 文件读取漏洞(CVE-2021-43798)

1) 漏洞描述

Grafana 是一个跨平台、开源的数据可视化网络应用程序平台。用户配置连接的数据源之后，Grafana 可以在网络浏览器里显示数据图表和警告。

Grafana 存在任意文件读取漏洞，攻击者可以读取服务器上任意文件，造成信息泄露。

2) 爆发时间

2021 年 12 月 7 日

3) 影响版本

8.0.0-beta1 <= Grafana <= 8.3.0

4) 检测规则

查看流量中是否存在类似 public/plugins/*/../ 路由（*为通配符）。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新至安全版本：

Grafana >= 8.3.1

下载地址：https://grafana.com/get/?plcmt=top-nav&cta=downloads

3.22 FineReport 文件上传漏洞（CNVD-2021-34467）

1) 漏洞描述

FineReport 是中国报表软件知名品牌，是帆软软件有限公司自主研发的一款企业级 web 报表软件产品。

FineReport 存在文件上传漏洞，攻击者可利用该漏洞上传任意文件，如木马文件，进而控制服务器。

2) 爆发时间

2021 年 6 月 11 日

3) 影响版本

FineReport 9.0

4) 检测规则

检查流量中是否有对 /WebReport/ReportServer?op=svginit&cmd=design_save_svg&filePath=chartmapsvg/../../../../WebReport/ 请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

漏洞已于 2021.4.8 发布版本修复：

下载地址：https://www.fanruan.com/support

3.23 H3C Intelligent Management Center 命令执行漏洞(CNVD-2021-39067)

1) 漏洞描述

H3C IMC（Intelligent Management Center）是 H3C 推出的下一代业务智能管理产品 1。H3C iMC (intelligent Management Center)是一个综合性的、模块化的平台，具有灵活性和可扩展性，可以满足中小型企业以及全球企业的网络需求。它整合了许多传统上分开管理的工具，包括管理网络基础设施、其服务和用户的工具。iMC 平台基于多年的积累和对网络的深入理解，为用户提供实用、易用的网络管理功能，包括拓扑、故障、性能、配置和安全等。

H3C Intelligent Management Center 存在命令执行漏洞。攻击者可利用漏洞通过构造特殊的请求造成远程命令执行。

2) 爆发时间

2021 年 7 月 3 日

3) 影响版本

H3C Intelligent Management Center

4) 检测规则

检查流量中是否有对 imc/javax.faces.resource/dynamiccontent.properties.xhtml 请求。

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

联系官方尽早升级到最新版本：https://www.h3c.com/cn/