斗象科技
TOPHANT

2023

HW 必修高危漏洞集合

版本：v1.0

2023.07

斗象科技 - 漏洞情报中心

Email: service@tophant.com

Tel: 400-156-9866

Tophant.com Freebuf.com Vulbox.com Tophant.ai

Make Security Entrenched Still | 让安全无法撼动

目录 CONTENTS

目录 CONTENTS

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

以下数据针对 22 年至今期间爆发的高危严重漏洞进行了数据统计和分析，具体的数据如下所示：

- 反序列化

  漏洞数量：3 个

  涉及厂商：Nacos、Apache Dubbo、Fastjson

- 逻辑漏洞

  漏洞数量：9 个

  涉及厂商：Smartbi、Grafana、Openfire、泛微、Apache、Spring、Linux

- 命令执行

  漏洞数量：15 个

  涉及厂商：Apache、nginxWebUI、畅捷通、Foxit、Smartbi、Weblogic、禅道、向日葵、F5 BIG-IP、Atlassian

- 其他

  漏洞类型包含：信息泄露、路径遍历、文件上传等

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
泛微 e-cology9 FileDownloadForOutDoc SQL 注入漏洞	SQL 注入	泛微	泛微 e-cology9 补丁版本 < 10.58
Smartbi 登录代码逻辑漏洞	逻辑漏洞	Smartbi	Smartbi >= V9
nginxWebUI 远程命令执行漏洞	命令执行	nginxWebUI	nginxWebUI <= 3.4.6
Smartbi 商业智能软件绕过登录漏洞	逻辑漏洞	Smartbi	V7 <= Smartbi <= V10

Openfire 身份认证绕过(CVE-2023-32315)	逻辑漏洞	Openfire	3.10.0 <= Openfire < 4.6.8 4.7.0 <= Openfire < 4.7.5
畅捷通 T+ 前台远程命令执行漏洞	命令执行	畅捷通	畅捷通 T+ 13.0 畅捷通 T+ 16.0
Nacos 反序列化漏洞	反序列化	Nacos	1.4.0 <= Nacos < 1.4.6 2.0.0 <= Nacos < 2.2.3
GitLab 路径遍历漏洞(CVE-2023-2825)	路径遍历	GitLab	GitLab CE 16.0.0 GitLab EE 16.0.0
Apache RocketMQ 命令注入漏洞(CVE-2023-33246)	命令执行	Apache	Apache RocketMQ 5.x < 5.1.1 Apache RocketMQ 4.x < 4.9.6
海康威视 iVMS-8700 综合安防管理平台软件 文件上传漏洞	文件上传	海康威视	iVMS-8700 V2.0.0 - V2.9.2 iSecure Center V1.0.0 - V1.7.0
泛微 e-cology9 用户登录漏洞	逻辑漏洞	泛微	泛微 e-cology9 补丁版本 < 10.57.2
Foxit PDF Reader/Editor exportXFAData 远程代码执行漏洞(CVE-2023-27363)	命令执行	Foxit	Foxit PDF Reader <= 12.1.1.15289 Foxit PDF Editor 12.x <= 12.1.1.15289 Foxit PDF Editor 11.x <= 11.2.5.53785 Foxit PDF Editor <= 10.1.11.37866
Apache bRPC 远程代码	命令执行	Apache	0.9.0 <= Apache bRPC <

执行漏洞 (CVE-2023-31039)			1.5.0
Grafana JWT 泄露漏洞 (CVE-2023-1387)	信息泄露	Grafana	9.1.0 <= Grafana < 9.2.17 9.3.0 <= Grafana < 9.3.13 9.4.0 <= Grafana < 9.5.0
Apache Superset 会话认证漏洞 (CVE-2023-27524)	逻辑漏洞	Apache	Apache Superset <= 2.0.1
Apache Druid 远程代码执行漏洞	命令执行	Apache	Apache Druid <= 25.0.0
Apache Solr 远程代码执行漏洞 (CNVD-2023-27598)	命令执行	Apache	8.10.0 <= Apache Solr < 9.2.0
MinIO 信息泄露 (CVE-2023-28432)	信息泄露	MinIO	RELEASE.2019-12-17T23-16-33Z <= MinIO < RELEASE.2023-03-20T20-16-18Z
Microsoft Outlook 特权提升漏洞 (CVE-2023-23397)	信息泄露	Microsoft	Microsoft Outlook 2016 (64-bit edition) Microsoft Outlook 2013 Service Pack 1 (32-bit editions) Microsoft Outlook 2013 RT Service Pack 1 Microsoft Outlook 2013 Service Pack 1 (64-bit editions) Microsoft Office 2019 for 32-bit editions

			Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office 2019 for 64-bit editions Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Office LTSC 2021 for 64-bit editions Microsoft Outlook 2016 (32-bit edition) Microsoft Office LTSC 2021 for 32-bit editions
Spring Framework 身份认证绕过漏洞 (CVE-2023-20860)	逻辑漏洞	Spring	Spring Framework 6.0.0 - 6.0.6 Spring Framework 5.3.0 - 5.3.25
Apache Dubbo 反序列化漏洞 (CVE-2023-23638)	反序列化	Apache	2.7.0 <= Apache Dubbo <= 2.7.21 3.0.0 <= Apache Dubbo <= 3.0.13 3.1.0 <= Apache Dubbo <= 3.1.5
Apache HTTP Server HTTP 请求走私漏洞 (CVE-2023-25690)	逻辑漏洞	Apache	Apache HTTP Server <= 2.4.55

Smartbi 远程命令执行漏洞	命令执行	Smartbi	V7<=Smartbi 大数据分析平台<= V10.5.8
Apache Kafka 远程代码执行漏洞 (CVE-2023-25194)	命令执行	Apache	Apache Kafka 2.3.0 - 3.3.2
Weblogic 远程代码执行漏洞 (CVE-2023-21839)	命令执行	Weblogic	WebLogic_Server = 12.2.1.3.0 WebLogic_Server = 12.2.1.4.0 WebLogic_Server = 14.1.1.0.0
禅道研发项目管理系统命令注入漏洞	命令执行	禅道	17.4 <= 禅道研发项目管理软件 <= 18.0.beta1 (开源版) 3.4 <= 禅道研发项目管理软件 <= 4.0.beta1(旗舰版) 7.4 <= 禅道研发项目管理软件 <= 8.0.beta1(企业版)
向日葵命令执行漏洞 (CNVD-2022-10270)	命令执行	向日葵	向日葵个人版 Windows <= 11.0.0.33 向日葵简约版 <= V1.0.1.43315(2021.12)
Linux DirtyPipe 权限提升漏洞 (CVE-2022-0847)	逻辑漏洞	Linux	Linux kernel>=5.8

Atlassian Bitbucker Data Center 远程代码执行漏洞 (CVE-2022-26133)	命令执行	Atlassian	Atlassian Bitbucket Data Center >= 5.14.x Atlassian Bitbucket Data Center 6.x Atlassian Bitbucket Data Center < 7.6.14 Atlassian Bitbucket Data Center < 7.16.x Atlassian Bitbucket Data Center < 7.17.6 Atlassian Bitbucket Data Center < 7.18.4 Atlassian Bitbucket Data Center < 7.19.4 Atlassian Bitbucket Data Center 7.20.0
Apache CouchDBi 权限提升漏洞 (CVE-2022-24706)	逻辑漏洞	Apache	Apache CouchDB <3.2.2
F5 BIG-IP 命令执行漏洞(CVE-2022-1388)	命令执行	F5 BIG-IP	16.1.0<=F5 BIG-IP<=16.1.2 15.1.0<=F5 BIG-IP<=15.1.5 14.1.0<=F5 BIG-IP<=14.1.4 13.1.0<=F5 BIG-IP<=13.1.4 12.1.0<=F5 BIG-IP<=12.1.6

			11.6.1<=F5 BIG-IP<=11.6.5
Fastjson 1.2.8 反序列化漏洞 (CVE-2022-25845)	反序列化	Fastjson	FastJson <= 1.2.80
Atlasssian Confluence OGNL 注入漏洞 (CVE-2022-26134)	命令执行	Atlasssian	Atlassian Confluence Server and Data Center >= 1.3.0 Atlassian Confluence Server and Data Center < 7.4.17 Atlassian Confluence Server and Data Center < 7.13.7 Atlassian Confluence Server and Data Center < 7.14.3 Atlassian Confluence Server and Data Center < 7.15.2 Atlassian Confluence Server and Data Center < 7.16.4 Atlassian Confluence Server and Data Center < 7.17.4 Atlassian Confluence Server and Data Center < 7.18.1

Apache Log4j2 远程代码执行漏洞（CVE-2021-44228）	远程代码执行	Apache Log4j2	Apache Log4j 2.x <= 2.14.1

三、 自查高危详情

3.1 泛微 e-cology9 FileDownloadForOutDoc SQL 注入漏洞

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 10.58.0 补丁之前存在 SQL 注入漏洞。未经授权的攻击者可以利用延时盲注进行 SQL 注入，从而获取数据库中的敏感信息。

2) 披露时间

2023 年 7 月 10 日

3) 影响版本

泛微 e-cology9 补丁版本 < 10.58

4) 检测规则

检查流量中是否有对 /weaver/weaver.file.FileDownloadForOutDoc 请求，且存在 SQL 注入相关的关键字

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：

泛微 e-cology9 补丁版本 >= 10.58.0

官方下载链接：https://www.weaver.com.cn/cs/securityDownload.html?src=cn

3.2 Smartbi 登录代码逻辑漏洞

1) 漏洞描述

Smartbi 大数据分析产品融合 BI 定义的所有阶段，对接各种业务数据库、数据仓库 和大数据分析平台，进行加工处理、分析挖掘和可视化展现；满足所有用户的各种数据 分析应用需求，如大数据分析、可视化分析、探索式分析、复杂报表、应用分享等。

Smartbi 在 V9 及其以上版本中存在登录代码逻辑漏洞，利用特定格式的 U RL 可以绕过登录校验代码，从而访问后台功能点

2) 披露时间

2023 年 7 月 3 日

3) 影响版本

Smartbi >= V9

4) 检测规则

查看流量设备中的 URL 是否存在 /vision/RMIServlet?windowUnloading 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补丁，请使用此产品的用户尽快更新安全补丁：

https://www.smartbi.com.cn/patchinfo

3.3 nginxWebUI 远程命令执行漏洞

1) 漏洞描述

nginxWebUI 是一款图形化管理 nginx 配置的工具，可以使用网页来快速配置 nginx 的各项功能，包括 http 协议转发、tcp 协议转发、反向代理、负载均衡、静态 html 服务器、ssl 证书自动申请、续签、配置等。配置好后可一键生成 nginx.conf 文件，同时可控制 nginx 使用此文件进行启动与重载，完成对 nginx 的图形化控制闭环。

nginxWebUI 存在未授权远程命令执行漏洞，攻击者可以直接在服务器上执行任意命令，甚至接管服务器

2) 披露时间

2023 年 6 月 28 日

3) 影响版本

nginxWebUI <= 3.4.6

4) 检测规则

查看流量设备中是否存在相关路由：/AdminPage/conf/runCmd?cmd=

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

nginxWebUI >= 3.4.7

3.4 Smartbi 商业智能软件 绕过登录漏洞

1) 漏洞描述

Smartbi 大数据分析产品融合 BI 定义的所有阶段，对接各种业务数据库、数据仓库和大数据分析平台，进行加工处理、分析挖掘和可视化展现；满足所有用户的各种数据分析应用需求，如大数据分析、可视化分析、探索式分析、复杂报表、应用分享等等。

Smartbi 商业智能软件在 V7-V10 版本存在登录绕过漏洞，某种特定情况下，默认用户绕过登录，从而在后台进行任意操作。

2) 披露时间

2023 年 6 月 16 日

3) 影响版本

V7 <= Smartbi <= V10

4) 检测规则

查看流量设备中 POST 请求的参数中是否存在 ["system","0a"] 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：https://www.smartbi.com.cn/patchinfo

3.5 Openfire 身份认证绕过(CVE-2023-32315)

1) 漏洞描述

Openfire 是一个基于 XMPP 协议的实时协作服务器，它是一个开源的项目，使用 Apache 许可证授权。它可以支持多种平台，提供强大的安全性和性能。XMPP 是一种开放的即时通讯协议，也叫做 Jabber。openfire 可以用来搭建聊天室，群组，视频会议等应用。Openfire 还提供了多种插件和扩展，以增强其功能和兼容性。

Openfire 在 3.10.0-4.6.7 和 4.7.0-4.7.4 版本中存在身份认证绕过漏洞，这允许未经身份验证的用户在已配置的 Openfire 环境中使用未经身份验证的 Openfire 安装环境，以访问 Openfire 管理控制台中为管理用户保留的受限页面。

2) 披露时间

2023 年 6 月 25 日

3) 影响版本

3.10.0 <= Openfire < 4.6.8

4.7.0 <= Openfire < 4.7.5

4) 检测规则

查看流量设备中 URL 中是否存在 /setup/setup-s/%u002e%u002e/%u002e%u002e/ 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

Openfire >= 4.6.8

Openfire >= 4.7.5

3.6 畅捷通 T+ 前台远程命令执行漏洞

1) 漏洞描述

畅捷通 T+是一款主要针对中小型工贸和商贸企业的财务业务一体化应用，融入了社交化、移动化、物联网、电子商务、互联网信息订阅等元素。

畅捷通 T+ 在 13.0 和 16.0 版本中存在 SQL 注入漏洞。未经授权的攻击者可以通过堆叠的方式进行命令执行漏洞。

2) 披露时间

2023 年 6 月 9 日

3) 影响版本

畅捷通 T+ 13.0

畅捷通 T+ 16.0

4) 检测规则

查看流量设备中是否存在对 /tplus/ajaxpro/Ufida.T.SM.UIP.MultiCompanyController,Ufida.T.SM.UIP.ashx?me thod=CheckMutex 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安全补丁：https://www.chanjetvip.com/product/goods/

3.7 Nacos 反序列化漏洞

1) 漏洞描述

Nacos 是一款开源的分布式服务发现和配置管理平台，用于帮助用户实现动态服务发现、服务配置管理、服务元数据及流量管理等功能。Nacos 在 1.4.0-1.4.5 和 2.0.0-2.2.2 版本中存在不安全的反序列化漏洞。Nacos 对部分 Jraft 请求处理时，使用 hessian 进行反序列化未限制而造成的 RCE 漏洞。

2) 披露时间

2023 年 6 月 6 日

3) 影响版本

1.4.0 <= Nacos < 1.4.6

2.0.0 <= Nacos < 2.2.3

4) 检测规则

查看流量设备中是否存在集群以外或陌生 IP 对 Nacos 的 7848(Raft 默认配置)端口 的连接。

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

Nacos >= 1.4.6

Nacos >= 2.2.3

下载地址：https://github.com/alibaba/nacos/releases

3.8 GitLab 路径遍历漏洞(CVE-2023-2825)

1) 漏洞描述

GitLab 是一个开源的代码托管平台。当嵌套在至少五个组中的公共项目中存在附件时，未经身份验证的恶意用户可以使用路径遍历漏洞读取服务器上的任意文件。

2) 披露时间

2023 年 5 月 24 日

3) 影响版本

GitLab CE 16.0.0

GitLab EE 16.0.0

4) 检测规则

查看流量中是否存在多个嵌套的组+../的关键字

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

GitLab CE 16.0.1

GitLab EE 16.0.1

下载地址：https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

3.9 Apache RocketMQ 命令注入漏洞 (CVE-2023-33246)

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。

Apache RocketMQ 在 5.1.1 和 4.9.6 版本之前存在命令注入漏洞。Apache RocketMQ 中的多个组件缺乏权限验证，攻击者可以通过使用更新配置功能，以 RocketMQ 运行的系统用户执行命令。此外，攻击者还可以通过伪造 RocketMQ 协议内容达到相同的利用效果。

2) 披露时间

2023 年 5 月 24 日

3) 影响版本

Apache RocketMQ 5.x < 5.1.1

Apache RocketMQ 4.x < 4.9.6

4) 检测规则

查看 RocketMQ 中的 broker 日志文件中更新配置参数是否存在恶意命令，如查找日志中 updateBrokerConfig, new config: 此行是否存在恶意命令

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

请使用此产品的用户尽快更新至安全版本

Apache RocketMQ 5.x >= 5.1.1

Apache RocketMQ 4.x >= 4.9.6

下载地址：https://rocketmq.apache.org/download/

3.10 海康威视 iVMS-8700 综合安防管理平台软件 文件上传漏洞

1) 漏洞描述

海康威视股份有限公司是一家专业从事视频监控产品的研发、生产和销售的高科技企业。

海康威视 iVMS-8700 综合安防管理平台软件存在文件上传漏洞。未经授权的 攻击者可以上传恶意 Webshell 文件，从而控制服务器

2) 披露时间

2023 年 5 月 19 日

3) 影响版本

iVMS-8700 V2.0.0 - V2.9.2

iSecure Center V1.0.0 - V1.7.0

4) 检测规则

检查流量中是否有对 /eps/api/resourceOperations/upload 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

详细修复方案请联系海康威视当地技术支持。

官方公告：https://www.hikvision.com/cn/support/CybersecurityCenter/SecurityNotices/2023-03/

6) 缓解措施

临时禁用上传接口

对接口进行鉴权

系统采用白名单校验

3.11 泛微 e-cology9 用户登录漏洞

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 10.57.2 补丁之前存在任意用户登录漏洞，攻击者可以利用信息泄露获取敏感信息，从而进行任意用户登录。

2) 披露时间

2023 年 5 月 17 日

3) 影响版本

泛微 e-cology9 补丁版本 < 10.57.2

4) 检测规则

检查流量中是否有对 /mobile/plugin/changeuserinfo.jsp 和/mobile/plugin/1/ofsLogin.jsp 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：

泛微 e-cology9 补丁版本 >= 10.57.2

官方下载链接：https://www.weaver.com.cn/cs/securityDownload.html?src=cn

3.12 Foxit PDF Reader/Editor exportXFAData 远程代码执行漏洞(CVE-2023-27363)

1) 漏洞描述

Foxit PDF Reader 是一个流行的 PDF 阅读软件，与 Adobe 的 PDF 软件相比，具有更快的速度和更小的体积。该软件存在一个远程代码执行（RCE）漏洞，由于在 exportXFAData 方法中暴露了一个可以写入任意文件的 JavaScript 接口，导致攻击者可以在受害者的系统中执行任意代码

2) 披露时间

2023 年 5 月 15 日

3) 影响版本

Foxit PDF Reader <= 12.1.1.15289

Foxit PDF Editor 12.x <= 12.1.1.15289

Foxit PDF Editor 11.x <= 11.2.5.53785

Foxit PDF Editor <= 10.1.11.37866

4) 检测规则

打开 C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup 查看是否存在恶意文件。

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：

Foxit PDF Reader >= 12.1.2.15332

Foxit PDF Editor >= 12.1.2.15332

官方下载链接：https://www.foxit.com/downloads/

3.13 Grafana JWT 泄露漏洞(CVE-2023-1387)

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。使用者组态连接的数据源之后，Grafana 可以在网络浏览器里显示数据图表和警告。

Grafana 是一个用于监控和可观察性的开源平台。从 9.1 分支开始，Grafana 引入了在 URL 查询参数 auth_token 中搜索 JWT 并将其用作身份验证令牌的功能。通过启用“url_login”配置选项（默认情况下禁用），可以将 JWT 发送到数据源。

2) 披露时间

2023 年 4 月 26 日

3) 影响版本

9.1.0 <= Grafana < 9.2.17

9.3.0 <= Grafana < 9.3.13

9.4.0 <= Grafana < 9.5.0

4) 检测规则

检查流量中是否有如下类似请求

```
curl -X POST -H "Content-Type: application/json" -d '{
  "client_id": "CLIENT_ID",
  "client_secret": "CLIENT_SECRET",
  "audience": "https://SUBDOMAIN.auth0.com/api/v2",
  "scope": "openid email read:email",
  "username": "USERNAME",
  "password": "PASSWORD",
  "grant_type": "http://auth0.com/oauth/grant-type/password-realm",
```

```
    "realm": "Username-Password-Authentication"
}' https://joaxcar.eu.auth0.com/oauth/token
```

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：

Grafana >= 9.2.17

Grafana >= 9.3.13

Grafana >= 9.5.0

官方下载链接：https://grafana.com/get/?plcmt=top-nav&cta=downloads

3.14 Apache Superset 会话认证漏洞 (CVE-2023-27524)

1) 漏洞描述

Apache Superset 是一个开源的数据探索和可视化平台。

如果没有根据安装说明更改默认配置的 SECRET_KEY ，将会允许攻击者验证和访问未经授权的资源。

这不会影响更改了 SECRET_KEY 配置默认值的 Superset 管理员。

2) 披露时间

2023 年 4 月 26 日

3) 影响版本

Apache Superset <= 2.0.1

4) 检测规则

检查配置是否使用了默认的 SECRET_KEY

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 Superset > 2.1.0

官方下载链接：https://superset.apache.org/docs/intro/

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。

6) 缓解措施

1. 创建一个文件 superset_config.py，并将其添加到 PYTHONPATH 中。

2. 在该文件中，设置一个强随机字符串作为 SECRET_KEY 的值，例如 `SECRET_KEY = 'YOUR_OWN_RANDOM_GENERATED_SECRET_KEY'`。可以使用 `openssl rand -base64 42` 命令生成一个强随机字符串。

3. 重启 Superset 服务，使配置生效。

3.15 Apache Druid 远程代码执行漏洞

1) 漏洞描述

Apache Druid 是一款分布式实时列存储系统，用于快速分析大规模数据集。

Apache Druid 存在远程代码执行漏洞，Apache Druid 受到 CVE-2023-25194 的影响，攻击者可以利用 CVE-2023-25194 使其进行 RCE 利用。

2) 披露时间

2023 年 4 月 19 日

3) 影响版本

Apache Druid <= 25.0.0

4) 检测规则

在流量探针中搜索是否存在访问路由：/druid/indexer/v1/sampler?for=connec，且 POST 中存在 ldap 关键字。

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) 缓解措施

druid 开启认证，参考链接：https://druid.apache.org/docs/latest/development/extensions-core/druid-basic-security.html

3.16 Apache Solr 远程代码执行漏洞 (CNVD-2023-27598)

1) 漏洞描述

Apache Solr 是一种开源的企业级搜索平台，用于快速和高效地搜索、索引和分析大量数据。

Apache Solr 在 8.10.0-9.2.0 之前的版本中存在远程代码执行漏洞。在 Apache Solr 开启 solrcloud 模式且其出网的情况下，未经授权的攻击者可以通过该漏洞进行 RCE 利用。

2) 披露时间

2023 年 4 月 17 日

3) 影响版本

8.10.0 <= Apache Solr < 9.2.0

4) 检测规则

检查流量中是否有对/solr/admin/configs?action=UPLOAD&name=exp&filePath=solrconfig.xml&overwrite=true 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：

Apache Solr >= 9.2.0

Apache Solr < 8.10.0

官方下载链接：https://github.com/apache/solr/releases/tag/releases

6) 缓解措施

1. 设置 solrcloud 模式机器进行不出网限制
2. 添加身份验证，不允许未授权使用 Solr 功能

3.17 MinIO 信息泄露(CVE-2023-28432)

1) 漏洞描述

MinIO 是在 GNU Affero 通用公共许可证 v3.0 下发布的高性能对象存储。它与 Amazon S3 云存储服务 API 兼容。使用 MinIO 为机器学习、分析和应用数据工作负载构建高性能基础架构。

MinIO 在 RELEASE.2019-12-17T23-16-33Z 至 RELEASE.2023-03-20T20-16-18Z 版本之前存在信息泄露，未经身份验证的攻击者向 MinIO 发送特制的 HTTP 请求可以获取 MINIO_SECRET_KEY、MINIO_ROOT_PASSWORD 等所有的环境变量。

2) 披露时间

2023 年 3 月 22 日

3) 影响版本

RELEASE.2019-12-17T23-16-33Z <= MinIO < RELEASE.2023-03-20T20-16-18Z

4) 检测规则

查看流量日志是否有以下路由访问记录 /minio/bootstrap/v1/verify

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：

MinIO >= RELEASE.2023-03-20T20-16-18Z

官方下载链接：https://github.com/minio/minio/tags

3.18 Microsoft Outlook 特权提升漏洞 (CVE-2023-23397)

1) 漏洞描述

Microsoft Office Outlook 是微软办公软件套装的组件之一，它对 Windows 自带的 Outlook express 的功能进行了扩充。Outlook 的功能很多，可以用它来收发电子邮件、管理联系人信息、记日记、安排日程、分配任务。

Microsoft Outlook 存在特权提升漏洞。攻击者可以通过发送特殊设计的电子邮件，该电子邮件在 Outlook 客户端进行检索和处理时会自动触发该漏洞利用，导致受害者会连接外部攻击者控制的 UNC，从而将受害者的 Net-NTLMv2 hash 值泄露给攻击者。

2) 披露时间

2023 年 3 月 15 日

3) 影响版本

Microsoft Outlook 2016 (64-bit edition)

Microsoft Outlook 2013 Service Pack 1 (32-bit editions)

Microsoft Outlook 2013 RT Service Pack 1

Microsoft Outlook 2013 Service Pack 1 (64-bit editions)

Microsoft Office 2019 for 32-bit editions

Microsoft 365 Apps for Enterprise for 32-bit Systems

Microsoft Office 2019 for 64-bit editions

Microsoft 365 Apps for Enterprise for 64-bit Systems

Microsoft Office LTSC 2021 for 64-bit editions

Microsoft Outlook 2016 (32-bit edition)

Microsoft Office LTSC 2021 for 32-bit editions

4) 检测规则

使用脚本检测与清理恶意邮件：https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/

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，根据对应版本更新对应补丁：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

6) 缓解措施

1. 将用户添加至 Protected Users Security 组，这可以有效阻止使用 NTLM 进行身份检验机制

2. 设置防火墙/VPN 阻止 TCP 445/SMB 出网，这可以阻止向远程文件共享发送 NTLM 身份验证信息

3.19 Spring Framework 身份认证绕过漏洞 (CVE-2023-20860)

1) 漏洞描述

Spring 框架是 Java 平台的一个开源的全栈（full-stack）应用程序框架和控制反转容器实现，一般被直接称为 Spring。该框架的一些核心功能理论上可用于任何 Java 应用，但 Spring 还为基于 Java 企业版平台构建的 Web 应用提供了大量的拓展支持。Spring 没有直接实现任何的编程模型，但它已经在 Java 社区中广为流行，基本上完全代替了企业级 JavaBeans（EJB）模型。

Spring Security 使用 "**" 作为匹配模式，同时配置 mvcRequestMatcher 会导致 Spring Security 和 Spring MVC 之间的模式不匹配，并可能存在身份认证绕过。

2) 披露时间

2023 年 3 月 22 日

3) 影响版本

Spring Framework 6.0.0 - 6.0.6

Spring Framework 5.3.0 - 5.3.25

4) 检测规则

检查 Spring Security 中 "**" 匹配模式是否与 mvcRequestMatcher 一同使用。

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 Framework >= 6.0.7

Spring Framework >= 5.3.26

官方下载链接：https://github.com/spring-projects/spring-framework/releases

6) 缓解措施

Spring Security 中 "**" 匹配模式不要与 mvcRequestMatcher 一同使用。

3.20 Apache Dubbo 反序列化漏洞(CVE-2023-23638)

1) 漏洞描述

Apache Dubbo 是一款易用、高性能的 WEB 和 RPC 框架，同时为构建企业级微服务提供服务发现、流量治理、可观测、认证鉴权等能力、工具与最佳实践。

dubbo 泛型调用存在反序列化漏洞，可导致恶意代码执行。

2) 披露时间

2023 年 3 月 8 日

3) 影响版本

2.7.0 <= Apache Dubbo <= 2.7.21

3.0.0 <= Apache Dubbo <= 3.0.13

3.1.0 <= Apache Dubbo <= 3.1.5

4) 检测规则

检查流量中是否有对外发起 LDAP 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：

Apache Dubbo >= 2.7.22

Apache Dubbo >= 3.0.14

Apache Dubbo >= 3.1.6

下载链接：https://mvnrepository.com/artifact/org.apache.dubbo/dubbo

3.21 Apache HTTP Server HTTP 请求走私漏洞 (CVE-2023-25690)

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。

当启用 mod_proxy 以及某种形式的 RewriteRule 或 ProxyPassMatch 时，配置会受到影响，其中非特定模式与用户提供的请求目标 (URL) 数据的某些部分匹配，然后使用重新插入代理请求目标变量替换。例如：

RewriteEngine on

RewriteRule "^/here/(.*)" " http://example.com:8080/elsewhere?$1" http://example.com:8080/elsewhere ; [P]

ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/

2) 披露时间

2023 年 3 月 8 日

3) 影响版本

Apache HTTP Server <= 2.4.55

4) 检测规则

检查流量中是否有 %20HTTP/1.1%0d%0aHost 相关请求

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：

Apache HTTP Server >= 2.4.56

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

3.22 Smartbi 远程命令执行漏洞

1) 漏洞描述

Smartbi 大数据分析产品融合 BI 定义的所有阶段，对接各种业务数据库、数据仓库和大数据分析平台，进行加工处理、分析挖掘和可视化展现；满足所有用户的各种数据分析应用需求，如大数据分析、可视化分析、探索式分析、复杂报表、应用分享等等。

Smartbi 大数据分析平台存在远程命令执行漏洞，攻击者可在服务器通过利用拼接、管

2) 披露时间

2023 年 3 月 1 日

3) 影响版本

V7<=Smartbi 大数据分析平台<= V10.5.8

4) 检测规则

检查流量中是否有对/smartbi/vision/RMIServlet

className=BIConfigService&methodName=testSmartbiXDataStorageConnection&params= 请求，且存在 ldap 注入相关的关键字，

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补丁版本：

补丁名称：修复了利用 stub 接口对"DB2 命令执行漏洞"补丁进行绕过的远

程命令执行漏洞

补丁链接：https://www.smartbi.com.cn/patchinfo

3.23 Apache Kafka 远程代码执行漏洞 (CVE-2023-25194)

1) 漏洞描述

Kafka 是由 Apache 软件基金会开发的一个开源流处理平台，由 Scala 和 Java 编写。该项目的目标是为处理实时数据提供一个统一、高吞吐、低延迟的平台。其持久化层本质上是一个“按照分布式事务日志架构的大规模发布/订阅消息队列”，这使它作为企业级基础设施来处理流式数据非常有价值。

此漏洞允许服务器连接到攻击者的 LDAP 服务器并反序列化 LDAP 响应，攻击者可以使用它在 Kafka 连接服务器上执行 java 反序列化小工具链。当类路径中有小工具时，攻击者可以造成不可信数据的无限制反序列化（或）RCE 漏洞。

此漏洞利用的前提是：需要访问 Kafka Connect worker，并能够使用任意 Kafka 客户端 SASL JAAS 配置和基于 SASL 的安全协议在其上创建/修改连接器。

自 Apache Kafka 2.3.0 以来，这在 Kafka Connect 集群上是可能的。

通过 Kafka Connect REST API 配置连接器时，经过身份验证的操作员可以将连接器的任何 Kafka 客户端的 `sasl.jaas.config` 属性设置为“com.sun.security.auth.module.JndiLoginModule”，它可以是通过“producer.override.sasl.jaas.config”、“consumer.override.sasl.jaas.config”或“admin.override.sasl.jaas.config”属性完成。

2) 披露时间

2023 年 2 月 7 日

3) 影响版本

Apache Kafka 2.3.0 - 3.3.2

4) 检测规则

访问 http://127.0.0.1:8083/connector-plugins 查看是否存在 io.debezium.connector.mysql 依赖且 kafka 版本在 2.3.0 - 3.3.2

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 Kafka >= 3.4.0

官方下载链接：https://kafka.apache.org/downloads

3.24 Weblogic 远程代码执行漏洞(CVE-2023-21839)

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。而此产品也延伸出 WebLogic Portal, WebLogic Integration 等企业用的中间件，以及 OEPE 开发工具。

WebLogic 存在远程代码执行漏洞，未经授权的攻击者利用此漏洞通告 T3、IIOP 协议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) 披露时间

2023 年 1 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。

5) 修复方案

厂商已发布了漏洞修复补丁，下载链接：https://support.oracle.com/rs?type=doc&id=2917213.2

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。

3.25 禅道研发项目管理系统命令注入漏洞

1) 漏洞描述

禅道研发项目管理软件是国产的开源项目管理软件,专注研发项目管理,内置需求管 理、任务管理、bug 管理、缺陷管理、用例管理、计划发布等功能,实现了软件的完整 生命周期管理。

禅道研发项目管理软件存在命令注入漏洞。 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) 披露时间

2023 年 1 月 6 日

3) 影响版本

17.4 <= 禅道研发项目管理软件 <= 18.0.beta1 (开源版)

3.4 <= 禅道研发项目管理软件 <= 4.0.beta1(旗舰版)

7.4 <= 禅道研发项目管理软件 <= 8.0.beta1(企业版)

4) 检测规则

检查流量中是否有对 /index.php?m=repo&f=edit&id= 的请求，且 POST 中存在 执行系统命令 相关的关键字。

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：

禅道研发项目管理软件 > 18.0.beta1 (开源版)

禅道研发项目管理软件 > 4.0.beta1(旗舰版)

禅道研发项目管理软件 > 8.0.beta1(企业版)

官方下载链接：https://www.zentao.net/

3.26 向日葵命令执行漏洞(CNVD-2022-10270)

1) 漏洞描述

向日葵是一款免费的集远程控制电脑手机、远程桌面连接、远程开机、远程管理、支持内网穿透的一体化远程控制管理工具软件。

向日葵简约版存在命令执行漏洞，攻击者可利用该漏洞获取服务器控制权

2) 披露时间

2023 年 2 月 13 日

3) 影响版本

向日葵个人版 Windows <= 11.0.0.33

向日葵简约版 <= V1.0.1.43315(2021.12)

4) 检测规则

检查流量中是否有对 /cgi-bin/rpc?action=verify-haras 和 /check?cmd=ping../../../../../../../../windows/system32 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：https://sunlogin.oray.com/

3.27 Linux DirtyPipe 权限提升漏洞(CVE-2022-0847)

1) 漏洞描述

CVE-2022-0847 是存在于 Linux 内核 5.8 及之后版本中的本地提权漏洞。攻击者通过利用此漏洞，可覆盖重写任意可读文件中的数据，从而可将普通权限的用户提升到特权 root。 CVE-2022-0847 的漏洞原理类似于 CVE-2016-5195 脏牛漏洞（Dirty Cow），但它更容易被利用。

2) 披露时间

2022 年 3 月 8 日

3) 影响版本

Linux kernel>=5.8

4) 检测规则

检查 Linux kernel 版本是否在影响范围内。

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

目前 Linux 内核官方已发布了解决上述漏洞的安全版本，建议受影响用户尽快进行安全更新。安全版本：- Linux 内核 >= 5.16.11- Linux 内核 >= 5.15.25- Linux 内核 >= 5.10.102

3.28 Atlassian Bitbucker Data Center 远程代码执行漏洞(CVE-2022-26133)

1) 漏洞描述

Atlassian 发布安全公告，修复了一个存在于 Atlassian Bitbucket Data Center 中的代码执行漏洞，漏洞编号：CVE-2022-26133，漏洞威胁等级：严重，漏洞评分：10.0。

该漏洞是由于 Atlassian Bitbucket Data Center 中的 Hazelcast 接口功能未对用户数据进行有效过滤，导致存在反序列化漏洞而引起的。攻击者利用该漏洞可以构造恶意数据远程执行任意代码。只有当 Atlassian Bitbucket Data Center 以 Cluster 模式安装时，才可能受该漏洞影响。

2) 披露时间

2022 年 4 月 27 日

3) 影响版本

Atlassian Bitbucket Data Center >= 5.14.x

Atlassian Bitbucket Data Center 6.x

Atlassian Bitbucket Data Center < 7.6.14

Atlassian Bitbucket Data Center < 7.16.x

Atlassian Bitbucket Data Center < 7.17.6

Atlassian Bitbucket Data Center < 7.18.4

Atlassian Bitbucket Data Center < 7.19.4

Atlassian Bitbucket Data Center 7.20.0

4) 检测规则

检查流量中是否有 ACED0005737200176A6176612E7574696C2E5072696F726

9747951756575659 4DA30B4FB3F82B10300024900047 3697A6 相关的关键字。

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

厂商已发布补丁修复漏洞，用户请尽快更新至安全版本：

7.6.14、7.17.6、7.18.4、7.19.4、7.20.1、7.21.0

如果您无法安装固定版本，可以通过以下方式自查 Bitbucket Data Center 是否是以 Cluster 模式安装的。打开 Bitbucket Data Center 的安装目录下的 confluence.cfg.xml 文件，若包含以下内容，则表明是以 Cluster 模式安装的。

<property name="confluence.cluster">true</property>

3.29 Apache CouchDBi 权限提升漏洞 (CVE-2022-24706)

1) 漏洞描述

Apache CouchDB 是美国阿帕奇（Apache）基金会的一个开源的面向文档的数据库管理系统，可以通过 RESTful JavaScript Object Notation (JSON) API 访问。

在 3.2.2 版本之前的 Apache CouchDB 中，可以在不进行身份验证的情况下访问不正确的默认安装并获得管理员权限：

1. CouchDB 打开一个随机网络端口，绑定到所有可用的接口以预期集群操作或 runtime introspection，称为 "epmd "的实用程序向网络公布了这个随机端口。epmd 本身在一个固定的端口上监听。

2. CouchDB 包装之前为单节点和集群安装选择了一个默认的"cookie "值，该 cookie 用于验证 Erlang 节点之间的任何通信。

2) 披露时间

2022 年 4 月 29 日

3) 影响版本

Apache CouchDB <3.2.2

4) 检测规则

查看 vm.args 中是否存在默认 cookie monster

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

厂商已发布补丁修复漏洞，用户请尽快更新至 Apache CouchDB 3.2.2 及更

高版本。下载链接：https://couchdb.apache.org/

CouchDB 3.2.2 及更高版本将拒绝使用以前默认的 Erlang cookie 值为`monster'，升级到此版本的安装将被迫选择不同的值。

此外，所有二进制包都已更新，以绑定`epmd`以及 CouchDB 分发端口分别为`127.0.0.1`和/或`::1`。

3.30 F5 BIG-IP 命令执行漏洞(CVE-2022-1388)

1) 漏洞描述

F5 BIG-IP iControl REST 存在命令执行漏洞 (CVE-2022-1388)。该漏洞允许远程未经身份验证的攻击者绕过 iControl REST 服务身份验证访问内部敏感服务进而执行任意命令。

攻击者可在应用处通过利用拼接、管道符、通配符等绕过手段来执行任意命令，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) 披露时间

2022 年 6 月 7 日

3) 影响版本

16.1.0<=F5 BIG-IP<=16.1.2

15.1.0<=F5 BIG-IP<=15.1.5

14.1.0<=F5 BIG-IP<=14.1.4

13.1.0<=F5 BIG-IP<=13.1.4

12.1.0<=F5 BIG-IP<=12.1.6

11.6.1<=F5 BIG-IP<=11.6.5

4) 检测规则

检查流量中是否有对 mgmt/tm/util/bash 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

升级到对应安全版本

补丁信息

补丁名称：F5 BIG-IP 安全漏洞的修复措施

补丁链接：https://support.f5.com/csp/article/K23605346

3.31 Fastjson 1.2.8 反序列化漏洞(CVE-2022-25845)

1) 漏洞描述

Fastjson 是阿里巴巴的开源 JSON 解析库，它可以解析 JSON 格式的字符串，支持将 Java Bean 序列化为 JSON 字符串，也可以从 JSON 字符串反序列化到 JavaBean。

在 Fastjson 1.2.80 及以下版本中存在反序列化漏洞，攻击者可以在特定依赖下利用此漏洞绕过默认 autoType 关闭限制，从而反序列化有安全风险的类。

2) 披露时间

2022 年 6 月 16 日

3) 影响版本

FastJson <= 1.2.80

4) 检测规则

检查流量中是否有 "@type": 相关请求。

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

官方已经发布修复链接，请及时下载并安装修复:https://github.com/alibaba/fastjson2/releases

版本升级

版本号：受影响用户请升级版本至 FastJson 1.2.83

版本链接：https://github.com/alibaba/fastjson/releases/tag/1.2.83

3.32 Atlasssian Confluence OGNL 注入漏洞 (CVE-2022-26134)

1) 漏洞描述

Atlassian Confluence 是 Atlassian 公司出品的专业 wiki 程序。它可以作为一个知识管理的工具，通过它能够实现团队成员之间的协作和知识共享。

2022 年 6 月 3 日，Atlassian 官方发布官方公告，披露存在 CVE-2022-26134 Confluence 远程代码执行漏洞在野攻击漏洞事件。漏洞利用无需身份认证，可直接前台远程执行任意代码。

2) 披露时间

2022 年 6 月 3 日

3) 影响版本

Atlassian Confluence Server and Data Center >= 1.3.0

Atlassian Confluence Server and Data Center < 7.4.17

Atlassian Confluence Server and Data Center < 7.13.7

Atlassian Confluence Server and Data Center < 7.14.3

Atlassian Confluence Server and Data Center < 7.15.2

Atlassian Confluence Server and Data Center < 7.16.4

Atlassian Confluence Server and Data Center < 7.17.4

Atlassian Confluence Server and Data Center < 7.18.1

4) 检测规则

检查流量中是否有对 /%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22 或其解码 /${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@ge

tRuntime().exec(" 请求。

5) 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。修复方案

官方已发布版本 7.4.17、7.13.7、7.14.3、7.15.2、7.16.4、7.17.4 和 7.18.1，其中包含对此漏洞的修复。请尽快升级到新版本

补丁信息

补丁名称：Atlassian Confluence Server 和 Data Center 远程代码执行漏洞的补丁

补丁链接：https://www.atlassian.com/software/confluence/download-archives

3.33 Apache Log4j2 远程代码执行漏洞 (CVE-2021-44228)

1) 漏洞描述

Apache Log4j 是一个基于 Java 的日志记录组件。Apache Log4j2 是 Log4j 的升级版本，通过重写 Log4j 引入了丰富的功能特性。该日志组件被广泛应用于业务系统开发，用以记录程序输入输出日志信息。

在特定的版本中由于其启用了 lookup 功能，从而导致产生远程代码执行漏洞。

2) 披露时间

2021 年 12 月 10 日

3) 影响版本

Apache Log4j 2.x <= 2.14.1

4) 检测规则

查看是否存在类似${jndi:相关请求流量。

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程序，请使用此产品的用户尽快更新至安全版本：

log4j >= 2.15.0-rc1

官方下载链接：https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1