亚信安全

2024年攻防演练

必修高危漏洞合集

-100+必修高危漏洞-

红队视角 筑牢攻防

亚信安全科技股份有限公司
应急响应中心

目录

1. 概述

随着网络安全的发展和攻防演练工作的推进，红蓝双方的技术水平皆在实践中得到了很大的提升，但是数字化快速发展也导致了企业的影子资产增多，企业很多老旧系统依旧存在历史漏洞，与此同时，在攻防演练期间，往往会爆出大量的0day漏洞，导致企业的防御体系被攻击队突破。

亚信安全结合自身的“外部攻击面管理”服务能力和专业的红队能力，以资产覆盖率、漏洞影响面、漏洞自动化利用指标为重点衡量参数，梳理了历史高危漏洞和近期爆发的漏洞共计118个，包括：远程代码执行、远程命令执行、反序列化、权限提升、认证绕过、SQL注入、未授权访问等漏洞。企业可以根据自身资产情况进行排查、补丁升级、防御策略优化等工作。

2. 漏洞详情

2.1 禅道项目管理系统身份认证绕过漏洞

➢ 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。

➢ 漏洞标签

服务器权限、国产开源框架、漏洞价值大、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

代码执行、权限绕过

➢ 检测规则

106058153、106058150

➢ 受影响版本

- 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)

➢ 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:

  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/

2.2 Primeton EOS Platform jmx 反序列化致远程代码执行漏洞

➢ 漏洞描述

Primeton EOS Platform 是普元信息技术股份有限公司推出的一款集成了低代码开发、微服务应用、开发运维一体化等功能的企业级应用开发平台。它能够帮助企业加快应用开发速度、提高运维效率，并提供灵活、可扩展的应用架构。

由于普元 EOS 某接口具备 JMX over HTTP 功能，且未对反序列化数据进行充分的安全检查和限制，攻击者可以通过利用反序列化漏洞，在服务器上执行任意代码，从而获得服务器的进一步控制权。最严重的情况下，这可能导致服务器的完全接管，敏感数据泄露，甚至将服务器转化为发起其他攻击的跳板。

➢ 漏洞标签

服务器权限、国产开源框架、影响范围广、红队打点必备

➢ 漏洞编号

暂无

➢ 漏洞类型

代码执行

➢ 检测规则

106058077

➢ 受影响版本

- Primeton EOS Platform<= 7.6

➢ 修复建议

- 目前，官方已有相关公告信息，建议获取最新补丁更新，需下载以下三个补丁更新：

  PLATFORM_V7_SERVER_20230725_P1

  3RD_SECURITY_20240125_C1

  3RD__COMMONS_COLLECTIONS_3.2_20151223_P1

- 官方下载链接：https://doc.primeton.com:29091/pages/viewpage.action?pageId=118129732

2.3 IP-guard WebServer 权限绕过漏洞

➢ 漏洞描述

IP-guard 是一款终端安全管理软件，旨在帮助企业保护终端设备安全、数据安全、管理网络使用和简化 IT 系统管理。

由于 IP-guard WebServer 的权限验证机制中存在设计缺陷，远程攻击者能够规避安全验证，通过后端接口执行文件的任意读取和删除操作。攻击者可利用该漏洞读取配置文件，造成敏感信息泄漏。

➢ 漏洞标签

影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

任意文件读取

➢ 检测规则

106058180

➢ 受影响版本

- IP-guard < 4.82.0609.0

➢ 修复建议

- 目前，官方已有相关公告信息，建议将 IP-guard 升级至 4.82.0609.0 及其版本以上；
- 官方下载链接：https://www.ip-guard.net/

2.4 泛微 E-Office10 反序列化漏洞

➢ 漏洞描述

泛微 E-Office10 是一款企业级办公自动化系统，主要用于优化和管理企业的文档、信息流转、协作与沟通工作流程。

由于系统处理上传的 PHAR 文件时存在缺陷，未经身份验证的远程攻击者能够上传伪装的恶意 PHAR 文件到服务器，从而在目标服务器上执行任意代码。

➢ 漏洞标签

服务器权限、漏洞价值大、红队打点必备

➢ 漏洞编号

暂无

➢ 漏洞类型

反序列化，代码执行

➢ 检测规则

103045083

➢ 受影响版本

- v10.0_20180516 < E-Office10 < v10.0_20240222

➢ 修复建议

- 目前，官方已发布新版本，建议访问官网获取版本升级安装包或补丁；
- 官方下载链接：https://www.e-office.cn/

2.5 Jenkins 任意文件读取漏洞

➢ 漏洞描述

Jenkins 是一个开源的基于 Java 开发的持续集成（CI）和持续交付（CD）工具，用于自动化构建、测试和部署软件项目。它提供了一个可扩展的平台，使开发团队能够集成和自动化各种工作流程，以减少手动操作和提高交付速度。

Jenkins 受影响版本中使用 args4j 库解析 CLI 命令参数，该库默认将参数中 @ 字符后的文件路径替换为文件内容，未授权的攻击者可利用该特性使用 Jenkins 控制器进程的默认字符编码读取 Jenkins 控制器文件系统上的任意文件(如加密密钥的二进制文件)，并结合 Resource Root URL、

Remember me cookie、存储型 XSS 或 CSRF 等在 Jenkins 控制器中执行任意代码。

- **漏洞标签**

服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

CVE-2024-23897

- **漏洞类型**

任意文件读取

- **检测规则**

106057106

- **受影响版本**

  - Jenkins weekly <= 2.441
  - Jenkins LTS <= 2.426.2

- **修复建议**

  - 禁用 Jenkins Cli，参考链接：https://github.com/jenkinsci-cert/SECURITY-3314-3315
  - 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：

    Jenkins weekly 2.442

    Jenkins LTS 2.426.3
  - 官方下载链接：

    https://github.com/jenkinsci/jenkins/commit/de450967f38398169650b55c002f1229a3fcdb1b

    https://github.com/jenkinsci/jenkins/commit/554f03782057c499c49bbb06575f0d28b5200edb

2.6 用友 YonBIP ServiceDispatcher 远程代码执行漏洞

- **漏洞描述**

用友 NC Cloud 是一种商业级的企业资源规划云平台，为企业提供全面的

管理解决方案，包括财务管理、采购管理、销售管理、人力资源管理等功能，实现企业的数字化转型和业务流程优化。

代码执行是指通过恶意输入或漏洞，将恶意代码注入到应用程序或系统中，从而执行未经授权的操作。这可能导致数据泄露、系统瘫痪或其他安全问题。

- **漏洞标签**

  漏洞价值大、红队打点必备 、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106053618、106053619

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：http://www.yonyou.com/

2.7 亿赛通电子文档安全管理系统 远程代码执行漏洞

- **漏洞描述**

  亿赛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。

亿赛通电子文档安全管理系统存在代码执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

- **漏洞标签**

  服务器权限、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106057793

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：https://www.esafenet.com

2.8 GitLab 任意用户密码重置漏洞

- **漏洞描述**

  GitLab 是由 GitLab 公司开发的、基于 Git 的集成软件开发平台。

  GitLab CE/EE 中支持用户通过辅助电子邮件地址重置密码，默认情况允许通过未经确认电子邮件重置密码。攻击者可以利用此漏洞将用户帐户密码重置电子邮件发送任意未经验证的电子邮件地址，导致用户帐户被接管。LDAP 用户不会受到影响。

- **漏洞标签**

  影响范围广、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2023-7028

- **漏洞类型**

  权限绕过

- **检测规则**

  106058029

- **受影响版本**

  - 16.1 <= Gitlab < 16.1.6
  - 16.2 <= Gitlab < 16.2.9
  - 16.3 <= Gitlab < 16.3.7
  - 16.4 <= Gitlab < 16.4.5
  - 16.5 <= Gitlab < 16.5.6
  - 16.6 <= Gitlab < 16.6.4
  - 16.7 <= Gitlab < 16.7.2

- **修复建议**

  - 官方已发布安全更新，建议升级至最新版本，若无法升级，建议利用安全组功能设置 Gitlab 仅对可信地址开放；
  - 官方下载链接：

    https://gitlab.com/gitlab-org/gitlab/-/commit/44deb06e2c8e1c1b9424fc89dec4f60c8806711a

2.9 kkFileView zipslip 远程代码执行漏洞

- **漏洞描述**

  kkFileView 是使用 spring boot 搭建的文件文档在线预览解决方案，支持主流办公文档的在线预览。

  kkFileView 4.2.0 到 4.4.0-beta 版本中文件上传功能存在 zip 路径穿越问题，导致攻击者可以通过上传恶意构造的 zip 包，覆盖任意文件。kkFileView 预览功能中会调用 Libreoffice 将 odt 文件转换为 pdf 文件，攻击者可通过覆盖该组件中的文件执行任意 python 代码。

- **漏洞标签**

  国产开源框架 、影响范围广、漏洞价值大、红队打点必备

➢ **漏洞编号**

暂无

➢ **漏洞类型**

文件上传，目录遍历

➢ **检测规则**

106057462

➢ **受影响版本**

- 4.2.0 <= kkFileView <= 4.4.0-beta

➢ **修复建议**

- 官方发布的最新版本中仍然存在此漏洞。用户可以通过从官方 GitHub 页面下载开发分支的最新代码来临时解决此问题。建议持续关注官方的版本更新通知，以便及时获得修复后的正式版本；
- 官方下载链接：https://github.com/kekingcn/kkFileView

2.10 Palo Alto Networks PAN-OS 命令注入漏洞

➢ **漏洞描述**

PAN-OS 是运行 Palo Alto Networks 下一代防火墙的软件。 通过利用 PAN-OS 本机内置的关键技术（App-ID、Content-ID、设备 ID 和用户 ID），可以在任何时间、任何地点完全了解和控制所有用户和设备中正在使用的应用程序。

Palo Alto Networks PAN-OS 软件的 GlobalProtect 功能中针对特定 PAN-OS 版本和不同功能配置下，未身份验证的攻击者可能利用此漏洞在防火墙上以 root 权限执行任意代码。

➢ **漏洞标签**

漏洞价值大、红队打点必备、涉及 HVV 重点系统

➢ **漏洞编号**

CVE-2024-3400

➢ **漏洞类型**

命令执行

- **检测规则**

106057465、106057405

- **受影响版本**

  - PAN-OS 11.1.* < 11.1.2-h3
  - PAN-OS 11.0.* < 11.0.4-h1
  - PAN-OS 10.2.* < 10.2.9-h1

- **修复建议**

  - 官方已对外发布安全更新补丁，建议受影响用户尽快升级。也可以利用安全组功能设置其仅对可信地址开放；
  - 官方下载链接：https://security.paloaltonetworks.com/CVE-2024-3400

2.11 用友 NC registerServlet 反序列化远程代码执行漏洞

- **漏洞描述**

用友 NC Cloud 是一种商业级的企业资源规划云平台，为企业提供全面的管理解决方案，包括财务管理、采购管理、销售管理、人力资源管理等功能，实现企业的数字化转型和业务流程优化。

用友 NC Cloud 存在反序列化代码执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

- **漏洞标签**

服务器权限、影响范围广 、漏洞价值大、红队打点必备

- **漏洞编号**

暂无

- **漏洞类型**

代码执行

- **检测规则**

106058181

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：http://www.yonyou.com/

2.12 亿赛通电子文档安全管理系统 hiddenWatermark/uploadFile 文件上传漏洞

- **漏洞描述**

  亿赛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。

  亿某通电子文档安全管理系统 hiddenWatermark/uploadFile 接口处存在文件上传漏洞，恶意攻击者可能上传恶意文件进而获取服务器的控制权限。恶意攻击者可以通过特定方式将文件上传到服务器的特定位置，获取系统权限，数据包中可能包含明显的目录遍历痕迹，如使用../等路径。攻击者通过这种方式尝试读取任意文件。

- **漏洞标签**

  服务器权限、漏洞价值大 、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  文件上传

- **检测规则**

106057793

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：https://www.esafenet.com

2.13 Atlassian Confluence template/aui/text-inline.vm 代码执行漏洞

- **漏洞描述**

  Confluence 是由 Atlassian 公司开发的企业协作和文档管理工具。

  Atlassian Confluence Data Center/Server 受影响版本中由于 velocity vm 模版可未授权访问，其中/aui/text-inline.vm 使用 findValue 解析 OGNL 表达式，表达式过滤不严，导致存在模版注入漏洞。攻击者可通过构造恶意请求，可以在未登录的情况下在 Confluence 实例上触发远程代码执行漏洞。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2023-22527

- **漏洞类型**

  代码执行

- **检测规则**

  106057541

- **受影响版本**

  - Atlassian Confluence Data Center and Server 8.0.x
  - Atlassian Confluence Data Center and Server 8.1.x
  - Atlassian Confluence Data Center and Server 8.2.x
  - Atlassian Confluence Data Center and Server 8.3.x

- Atlassian Confluence Data Center and Server 8.4.x
- Atlassian Confluence Data Center and Server 8.5.0-8.5.3

➢ **修复建议**

- 目前，官方已发布新版本，请将组件 confluence_server 升级至 8.5.4 及以上版本，将组件 confluence_data_center 升级至 8.5.4 及以上版本；
- 官方下载链接：https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

2.14 亿赛通电子文档安全管理系统 AutoSignService1 接口远程代码执行漏洞

➢ **漏洞描述**

亿赛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。

亿赛通电子文档安全管理系统存在代码执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

➢ **漏洞标签**

服务器权限、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

➢ **漏洞编号**

暂无

➢ **漏洞类型**

代码执行

- **检测规则**

  106058182

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：https://www.esafenet.com

2.15 亿赛通电子文档安全管理系统 CDG AuthoriseTempletService1 接口远程代码执行漏洞

- **漏洞描述**

  亿赛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。

  亿赛通电子文档安全管理系统存在代码执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

- **漏洞标签**

  服务器权限、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

106058183

- **受影响版本**

  暂无

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：https://www.esafenet.com

2.16 堡塔云 WAF get_site_status 路径 server_name 参数 SQL 注入漏洞

- **漏洞描述**

  堡塔云 WAF（Web Application Firewall）是广东堡塔安全技术有限公司的一款基于云计算的 Web 应用防火墙解决方案。它通过监控和过滤 Web 应用程序的流量，识别和阻止潜在的网络攻击，并保护 Web 应用程序免受恶意行为和漏洞利用的威胁。

  堡塔云 WAF get_site_status 接口 server_name 参数存在 SQL 注入漏洞，攻击者可利用此漏洞获取数据库敏感信息。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  106057787

- **受影响版本**

  暂无

- **修复建议**

- 厂商已提供修复版本；
- 官方下载链接：https://www.bt.cn/

2.17 Weblogic ForeignOpaqueReference 远程代码执行漏洞（CVE-2024-20931）

➢ 漏洞描述

Oracle WebLogic Server 是一个用于构建、部署和管理企业级 Java 应用程序。AQjmsInitialContextFactory 是一个允许应用程序使用 JNDI 查找方式访问 Oracle AQ 提供消息服务的工厂类。ForeignOpaqueReference 是一个对象，lookup 时会调用 getReferent 函数，进行远程对象查询。

该漏洞是 CVE-2023-21839 漏洞绕过，在 AQjmsInitialContextFactory 初始化时会通过 JNDI 获取远程的 DataSource，当通过反射修改 ForeignOpaqueReference 的 jndiEnvironment 和 remoteJNDIName 属性后，再次远程查询 ForeignOpaqueReference 对象会导致 JNDI 注入，从而直接接管 Oracle WebLogic Server 来执行未经授权的操作或访问系统敏感信息。

➢ 漏洞标签

服务器权限、工具/武器化成熟、影响范围广、漏洞价值大、历史重大漏洞

➢ 漏洞编号

CVE-2024-20931

➢ 漏洞类型

代码执行

➢ 检测规则

103045134

➢ 受影响版本

- weblogic_server14.1.1.0.0, 14.1.1.0.0
- weblogic_server12.2.1.4.0, 12.2.1.4.0

➢ 修复建议

- 安装官方 1 月补丁；

- 官方下载链接：https://www.oracle.com/security-alerts/cpujan2024.html

2.18 飞鱼星企业级智能上网行为管理系统 /send_order.cgi?parameter=operation 命令执行漏洞

➢ 漏洞描述

飞鱼星企业级智能上网行为管理系统是成都飞鱼星科技开发有限公司开发的一款上网行为管理路由器，专为中小企业、政府机关、教育及科研机构等用户设计，是具备“上网行为管理”、“多 WAN 路由器”以及“VPN 网关”多重功能的新一代硬件网络接入设备。它能帮助企业对员工使用因特网的情况进行监控、生成报表并进行管理；帮助企业提高员工的生产率、节省网络带宽并且减少法律风险。

飞鱼星企业级智能上网行为管理系统 send _order.cgi 接口处存在远程命令执行漏洞，未经身份验证的攻击者可以利用此漏洞执行任意指令，且写入后门文件可获取服务器权限，造成严重威胁。

➢ 漏洞标签

服务器权限 、漏洞价值大、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

命令执行

➢ 检测规则

106057726

➢ 受影响版本

暂无

➢ 修复建议

- 关闭互联网暴露面或接口设置访问权限；
- 升级至安全版本，详见官网：http://www.adslr.com/products/19.html

2.19 畅捷通 T+ /tplus/UFAQD/InitServerInfo.aspx SQL 注入漏洞

➢ 漏洞描述

T+是用友畅捷通推出的一款新型互联网企业管理系统，T+能够满足成长型小微企业对其灵活业务流程的管控需求，重点解决往来业务管理、订单跟踪、资金、库存等管理难题。用户可以通过各种固定或移动设备随时随地迅速获取企业实时、动态的运营信息。

畅捷通 T+InitServerInfo.aspx 接口处存在 SQL 注入漏洞 ，恶意攻击者可能会利用该漏洞获取服务器敏感信息，最终可能导致服务器失陷。

➢ 漏洞标签

服务器权限、漏洞价值大、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

SQL 注入

➢ 检测规则

106057755

➢ 受影响版本

- 畅捷通 T+ 13.0
- 畅捷通 T+ 16.0

➢ 修复建议

- 厂商已提供修复版本；
- 官方下载链接：https://www.chanjet.com/

2.20 D-Link NAS /cgi-bin/nas_sharing.cgi 命令执行漏洞

➢ 漏洞描述

D-Link DNS-320 是中国友讯（D-Link）公司的一款 NAS（网络附属存储）设备。

D-Link DNS-320L 存在命令注入漏洞，该漏洞源于文件/cgi-bin/nas_sharing.cgi 存在命令注入漏洞。受影响的是组件 HTTP GET Request Handler 的文件/cgi-bin/nas_sharing.cgi 中的一个未知功能。对参数 system 的篡改导致命令注入。攻击者可以远程发动攻击。

- **漏洞标签**

  服务器权限、漏洞价值大、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2024-3273

- **漏洞类型**

  命令执行

- **检测规则**

  106058149

- **受影响版本**

  - DNS-320L
  - DNS-325
  - DNS-327
  - DNS-340L
  - D-Link NAS Storage

- **修复建议**

  - 供应商早期已被联系并立即确认该产品已达到生命周期终点，应该退役并更换；
  - 此漏洞仅影响不再得到维护的产品。建议更新当前系统或软件至最新版，完成漏洞的修复；
  - 官方链接：http://www.dlink.com.cn/

2.21 致远互联 FE /sysform/003/editflow_manager.jsp SQL 注入漏洞

- **漏洞描述**

  致远互联 FE 协作办公平台是一款为企业提供全方位协同办公解决方案的产品。它集成了多个功能模块，旨在帮助企业实现高效的团队协作、信息共享和文档管理。

  致远互联 FE 协作办公平台 editflow_manager 存在 SQL 注入漏洞，由于 GUID 参数未过滤或者过滤不严格，攻击者可以获得敏感信息。

- **漏洞标签**

  漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  106057909

- **受影响版本**

  暂无

- **修复建议**

  - 部署 Web 应用防火墙，对数据库操作进行监控；
  - 升级至系统最新版本；
  - 官方下载链接：https://www.seeyon.com/

2.22 Jeecg /api/../commonController.do 文件 文件上传漏洞

- **漏洞描述**

  Jeecg (J2EE C ode G eneration)是一款基于代码生成器的低代码开发平台，使用 JEECG 可以简单快速地开发出企业级的 Web 应用系统。目前官方已停止维护。

  由于/api 接口鉴权时未过滤路径遍历，攻击者可构造包含../的 url 绕过鉴

权。攻击者可构造恶意请求利用 commonController 接口进行文件上传攻击实现远程代码执行，导致服务器被控。

- **漏洞标签**

服务器权限、国产开源框架 、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

文件上传

- **检测规则**

106057674

- **受影响版本**

  - JEECG 4.0 及之前版本

- **修复建议**

  - 官方已停止维护，建议利用安全组设置其仅对可信地址开放。

2.23 锐捷 RG-EW1200G /api/sys/login 权限绕过漏洞

- **漏洞描述**

Ruijie Networks RG-EW1200G 是中国锐捷网络（Ruijie Networks）公司的一款无线路由器。

Ruijie Networks RG-EW1200G 存在授权问题漏洞，该漏洞源于文件 /api/sys/login 存在不当的身份验证。

- **漏洞标签**

红队打点必备、漏洞价值大 、影响范围广

- **漏洞编号**

CVE-2023-4415

- **漏洞类型**

权限绕过

- **检测规则**

106047703

- **受影响版本**

  - 07161417_r483<=rg-ew1200g_firmware<=07161417_r483

- **修复建议**

  - 厂商已提供修复版本；
  - 官方下载链接：https://www.ruijie.com.cn/

2.24 畅捷通 T+ /tplus/UFAQD/KeyInfoList.aspx SQL 注入漏洞

- **漏洞描述**

T+是用友畅捷通推出的一款新型互联网企业管理系统，T+能够满足成长型小微企业对其灵活业务流程的管控需求，重点解决往来业务管理、订单跟踪、资金、库存等管理难题。用户可以通过各种固定或移动设备随时随地迅速获取企业实时、动态的运营信息。

由于畅捷通 T＋的 KeyInfoList. aspx 接口处未对用户的输入进行过滤和校验， 未经身份验证的攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

- **漏洞标签**

服务器权限、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

SQL 注入

- **检测规则**

106058184

- **受影响版本**
  - 畅捷通 T+ 13.0
  - 畅捷通 T+ 16.0
- **修复建议**
  - 厂商已提供修复版本；
  - 官方下载链接：https://www.chanjet.com/

2.25 Fortinet FortiOS 代码执行漏洞

➢ 漏洞描述

Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web 内容过滤和反垃圾邮件等多种安全功能。

Fortinet FortiOS 存在缓冲区错误漏洞，该漏洞源于存在越界写入，允许攻击者通过特制请求执行未经授权的代码或命令。

➢ 漏洞标签

影响范围广、漏洞价值大、涉及 HVV 重点系统

➢ 漏洞编号

CVE-2024-21762

➢ 漏洞类型

代码执行

➢ 检测规则

106058192

➢ 受影响版本

- 1.0.0<=fortiproxy<2.0.14
- 7.0.0<=fortiproxy<7.0.15
- 7.2.0<=fortiproxy<7.2.9
- 7.4.0<=fortiproxy<7.4.3
- 6.0.0<=fortios<6.2.16

- 6.4.0<=fortios<6.4.15
- 7.0.0<=fortios<7.0.14
- 7.2.0<=fortios<7.2.7
- 7.4.0<=fortios<7.4.3

➢ **修复建议**

- 目前官方已发布安全更新，受影响用户可以更新到最新版本：

  将 6.2.x 版本 fortios 升级至 6.2.16 及以上版本

  将 6.4.x 版本 fortios 升级至 6.4.15 及以上版本

  将 7.0.x 版本 fortios 升级至 7.0.14 及以上版本

  将 7.2.x 版本 fortios 升级至 7.2.7 及以上版本

  将 7.4.x 版本 fortios 升级至 7.4.3 及以上版本

  将组件 fortiproxy 升级至 2.0.14/7.0.15/7.2.9/7.4.3 及以上安全版本

- 官方下载链接：https://fortiguard.com/psirt/FG-IR-24-015

2.26 Jeecg jeecgFormDemoController JNDI 代码执行漏洞

➢ **漏洞描述**

Jeecg (J2EE C ode G eneration)是一款基于代码生成器的低代码开发平台，使用 JEECG 可以简单快速地开发出企业级的 Web 应用系统。目前官方已停止维护。

JEECG 4.0 及之前版本中，由于 /api 接口鉴权时未过滤路径遍历，攻击者可构造包含 ../ 的 url 绕过鉴权。因为依赖 1.2.31 版本的 fastjson，该版本存在反序列化漏洞。攻击者可对 /api/../jeecgFormDemoController.do?interfaceTest 接口进行 jndi 注入攻击实现远程代码执行。

➢ **漏洞标签**

服务器权限 、国产开源框架 、漏洞价值大、涉及 HVV 重点系统

➢ **漏洞编号**

CVE-2023-49442

➢ **漏洞类型**

代码执行

- **检测规则**

106058038

- **受影响版本**

  - JEECG 4.0 及之前版本

- **修复建议**

  - 官方已停止维护，建议利用安全组设置其仅对可信地址开放。

2.27 金蝶 Apusic loadTree 存在 JNDI 注入

- **漏洞描述**

金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。

金蝶 Apusic 应用服务器 存在 JNDI 注入漏洞，由于金蝶 Apusic 应用服务器权限验证不当，导致攻击者可以向 createDataSource 接口执行 JNDI 注入，造成远程代码执行漏洞。利用该漏洞需低版本 JDK 且需要服务器上有数据库驱动。

- **漏洞标签**

影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

代码执行

- **检测规则**

106054216

- **受影响版本**

  - 金蝶 Apusic 应用服务器 <= V9.0 SP7

- **修复建议**

  - 官方已发布补丁修复漏洞，建议尽快安装补丁修复漏洞；

- 官方补丁下载地址：http://file.apusic.com/sharing/vVHoyV0jR

2.28 金蝶 Apusic deployApp 任意文件上传漏洞

➢ 漏洞描述

金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。

金蝶 Apusic 应用服务器 deployApp 接口存在任意文件上传漏洞，攻击者可在未授权的情况下利用此漏洞绕过鉴权上传任意文件，最终可能导致远程执行恶意命令，控制服务器。

➢ 漏洞标签

服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

文件上传

➢ 检测规则

106057725

➢ 受影响版本

- Apusic 应用服务器 < V9.0 SP8

➢ 修复建议

- 目前官方已经发布补丁，建议受影响用户尽快安装补丁；
- 官方下载链接：https://www.apusic.com/view-477-113.html

2. 29 Apache Struts2 目录遍历漏洞

➢ 漏洞描述

Apache Struts 2 是一个用于开发 Java EE 网络应用程序的开放源代码网页

应用程序架构。它利用并延伸了 Java Servlet API，鼓励开发者采用 MVC 架构。

由于 Struts 框架在处理参数名称大小写方面的不一致性，导致未经身份验证的远程攻击者能够通过修改参数名称的大小写来利用目录遍历技术上传恶意文件到服务器的非预期位置，最终导致代码执行。

- **漏洞标签**

  开源框架、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2023-50164

- **漏洞类型**

  目录遍历

- **检测规则**

  103046166

- **受影响版本**

  - 2.5.0 <= Struts <= 2.5.32
  - 6.0.0 <= Struts <= 6.3.0
  - 2.0.0 <= Struts <= 2.3.37 (EOL)

- **修复建议**

  - 目前，官方已有可更新版本，建议用户尽快更新到安全版本：

    Struts >= 2.5.33

    Struts >= 6.3.0.2

  - 官方下载链接：
    https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lfwtqhj

2.30 金蝶云星空 /ScpSupRegHandler 路径存在任意文件上传漏洞

- **漏洞描述**

  金蝶云星空是金蝶软件推出的一款云计算平台，旨在为企业提供全面的云服务和解决方案。它将金蝶软件丰富的企业管理应用和云计算技术相结合，

帮助企业实现数字化转型和业务的快速发展。

金蝶云星空私有云存在任意文件上传漏洞，攻击者可在未授权的情况下利用此漏洞上传任意文件，最终可能导致远程执行恶意命令，控制服务器。

➢ 漏洞标签

服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

文件上传

➢ 检测规则

106053018

➢ 受影响版本

- 金蝶云星空企业版私有云、企业版私有云（订阅）、标准版私有云（订阅）三个产品
- 涉及版本：V6.2(含 17 年 12 月补丁) 至 V8.1(含 23 年 9 月补丁)

➢ 修复建议

- 目前官方已经发布补丁，建议受影响用户尽快安装补丁；
- 官方下载链接：https://vip.kingdee.com/school/detail/505412093244235264?productLineId=1
- 若客户暂时无法升级，应避免将受影响系统对公司访问，可通过设置网络 ACL 策略限制访问来源，例如只允许特定 IP 地址或地址段的访问。

2.31 Atlassian Confluence 远程代码执行漏洞

➢ 漏洞描述

Confluence 是由 Atlassian 公司开发的企业协作和文档管理工具。

Atlassian Confluence Data Center & Server 中存在授权不当漏洞，未经身份认证的远程攻击者可能利用此漏洞破坏服务端的可用性及完整性。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2023-22518

- **漏洞类型**

  代码执行，权限绕过

- **检测规则**

  106053637

- **受影响版本**

  - Atlassian Confluence Data Center & Server < 7.19.16
  - Atlassian Confluence Data Center & Server < 8.3.4
  - Atlassian Confluence Data Center & Server < 8.4.4
  - Atlassian Confluence Data Center & Server < 8.5.3
  - Atlassian Confluence Data Center & Server < 8.6.1

  注：目前已经停止维护的版本同样受此漏洞影响。

- **修复建议**

  - 目前，Atlassian 官方已发布可更新版本，建议受影响用户升级至：

    Atlassian Confluence >= 7.19.16

    Atlassian Confluence >= 8.3.4

    Atlassian Confluence >= 8.4.4

    Atlassian Confluence >= 8.5.3

    Atlassian Confluence >= 8.6.1

  - 官方下载链接：

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

2.32 F5 BIG-IP TMUI 远程代码执行漏洞

- **漏洞描述**

  F5 BIG-IP 是 F5 公司一款集成了网络流量编排、负载均衡、智能 DNS，远

程接入策略管理等功能的应用交付平台。

F5 BIG-IP 存在远程代码执行漏洞，该漏洞是由配置实用程序身份验证绕过缺陷引起的。攻击者可利用该漏洞在系统上执行任意系统命令。

- **漏洞标签**

影响范围广、漏洞价值大、红队打点必备、软件供应链风险、涉及 HVV 重点系统

- **漏洞编号**

CNVD-2023-82300

- **漏洞类型**

代码执行

- **检测规则**

106052576

- **受影响版本**

  - 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

- **修复建议**

  - 目前官方已经发布补丁，建议受影响用户尽快安装补丁；
  - 官方下载链接：https://my.f5.com/manage/s/article/K000137353

2.33 Apache ActiveMQ 服务端口 远程代码执行漏洞

- **漏洞描述**

ActiveMQ 是一个开源的消息代理和集成模式服务器，它支持 Java 消息服务(JMS)API。它是 Apache Software Foundation 下的一个项目，用于实现消息中间件，帮助不同的应用程序或系统之间进行通信。

Apache ActiveMQ 中存在远程代码执行漏洞， Apache ActiveMQ 在默认安装下开放了 61616 服务端口，而该端口并没有对传入数据进行适当的过

滤，从而使攻击者能够构造恶意数据以实现远程代码执行。

- **漏洞标签**

开源框架、工具/武器化成熟、影响范围广、软件供应链风险 、涉及 HVV 重点系统

- **漏洞编号**

CNVD-2023-69477

- **漏洞类型**

代码执行

- **检测规则**

106058036

- **受影响版本**

  - Apache ActiveMQ <5.18.3
  - Apache ActiveMQ <5.17.6
  - Apache ActiveMQ<5.16.7
  - Apache ActiveMQ<5.15.16

- **修复建议**

  - 目前官方已通过限制反序列化类只能为 Throwable 的子类的方式来修复此漏洞。建议受影响用户可以更新到：

    Apache ActiveMQ >= 5.18.3

    Apache ActiveMQ >= 5.17.6

    Apache ActiveMQ >= 5.16.7

    Apache ActiveMQ >= 5.15.16

  - 官方下载链接：https://github.com/apache/activemq/tags

2.34 金山终端安全系统 V9.0 SQL 注入漏洞

- **漏洞描述**

金山终端安全系统是一款为企业提供终端防护的安全产品，针对恶意软件、病毒和外部攻击提供防范措施，帮助维护企业数据和网络。

2023 年 10 月，互联网上披露其存在前台 SQL 注入漏洞，攻击者可利用 SQL 注入达到文件写入，从而实现远程代码执行，控制服务器。

- **漏洞标签**

  服务器权限 、影响范围广 、漏洞价值大、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  106057821

- **受影响版本**

  - 金山终端安全系统<V9.SP1.E1008

- **修复建议**

  - 目前官方已经发布补丁，建议用户升级至 V9.SP1.E1008 及其以上版本；
  - 官方下载链接：https://www.ejinshan.net/lywz/index

2.35 金蝶 EAS /myUploadFile.do 路径存在任意文件上传漏洞

- **漏洞描述**

  金蝶云星空是金蝶软件推出的一款云计算平台，旨在为企业提供全面的云服务和解决方案。它将金蝶软件丰富的企业管理应用和云计算技术相结合，帮助企业实现数字化转型和业务的快速发展。

  金碟 EAS myUploadFile.do 接口处存在任意文件上传漏洞，攻击者可以通过构造特殊请求包上传恶意后门文件，从而获取服务器权限。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

  文件上传

- **检测规则**

  106057952

- **受影响版本**

  - 金蝶 EAS 8.0，8.1，8.2，8.5
  - 金蝶 EAS Cloud 8.6 私有云，8.6 公有云，8.6.1，8.8

- **修复建议**

  - 目前官方已经发布补丁，建议受影响用户尽快安装补丁。
  - 官方下载链接：https://www.kingdee.com/products/eascloud.html

2.36 Citrix ADC & Citrix Gateway 会话令牌泄漏漏洞

- **漏洞描述**

  Citrix NetScaler Gateway（以前称为 Citrix Gateway）和 NetScaler ADC（以前称为 Citrix ADC）都是 Citrix 公司的产品。Citrix NetScaler Gateway 是一套安全的远程接入解决方案。该方案可为管理员提供应用级和数据级管控功能，以实现用户从任何地点远程访问应用和数据。Citrix Systems NetScaler ADC 是一个应用程序交付和安全平台。

  NetScaler ADC 和 NetScaler Gateway 上存在代码注入漏洞，相邻网络上具有低权限的攻击者可通过管理界面访问 NSIP、CLIP 或 SNIP 后利用该漏洞在系统上执行代码。由于处理/oauth/idp/.well-known/openid-configuration 函数时，请求头多次拷贝超出 print_temp_rule 缓冲区的大小，导致缓冲区溢出，产生内存泄漏。当 NetScaler ADC 和 NetScaler Gateway 配置为网关（VPN 虚拟服务器，ICA 代理，CVPN，RDP 代理）或 AAA 虚拟服务器时，未经身份验证的攻击者可以利用内存泄漏劫持用户的 session，绕过身份验证，获取敏感信息。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、软件供应链风险、涉及 HVV 重点系统

➢ **漏洞编号**

CVE-2023-4966

➢ **漏洞类型**

权限绕过

➢ **检测规则**

106058024

➢ **受影响版本**

- NetScaler ADC and NetScaler Gateway 14.1.x < 14.1-12.35
- NetScaler ADC and NetScaler Gateway 13.1.x <13.1-51.15
- NetScaler ADC and NetScaler Gateway 13.0.x < 13.0-92.21
- NetScaler ADC 13.1-FIPS.x < 13.1-37.176
- NetScaler ADC 12.1-FIPS.x < 12.1-55.302
- NetScaler ADC 12.1-NDcPP.x < 12.1-55.302

注意：NetScaler ADC 和 NetScaler Gateway 版本 12.1 现已停产（EOL），并且容易受到攻击。

➢ **修复建议**

- 目前，Citrix 官方已发布漏洞修复补丁，建议受影响用户升级至：

  NetScaler ADC and NetScaler Gateway 14.1.x >= 14.1-12.35

  NetScaler ADC and NetScaler Gateway 13.1.x >=13.1-51.15

  NetScaler ADC and NetScaler Gateway 13.0.x >= 13.0-92.21

  NetScaler ADC 13.1-FIPS.x >= 13.1-37.176

  NetScaler ADC 12.1-FIPS.x >= 12.1-55.302

  NetScaler ADC 12.1-NDcPP.x >= 12.1-55.302

- 官方下载链接：

  https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549

2.37 泛微 E-Office 10

/eoffice10/server/public/api/welink/welink-move 远程代码执行漏洞

- **漏洞描述**

  泛微 E-Office10 是一款企业级办公自动化系统，主要用于优化和管理企业的文档、信息流转、协作与沟通工作流程。

  在受影响版本中，由于处理上传的 phar 文件时存在缺陷，攻击者可向 /eoffice10/server/public/api/welink/welink-move 等地址上传恶意 phar 文件，利用针对 phar 的反序列化触发远程代码执行。

- **漏洞标签**

  影响范围广、漏洞价值大、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行，文件上传

- **检测规则**

  106047789

- **受影响版本**

  - E-office10<10.0_20240222

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网获取版本升级安装包或补丁；
  - 官方下载链接：https://www.e-office.cn/

2.38 用友 GRP-U8 /u8qx/bx_historyDataCheck.jsp SQL 注入漏洞

- **漏洞描述**

  用友 GRP-U8 行政事业财务管理软件是用友公司专注于国家电子政务事业，基于云计算技术所推出的新一代产品。

在用友 GRP-U8 的 bx_historyDataCheck jsp 存在 SQL 注入漏洞，由于用友 GRP-U8 未对用户的输入进行有效的过滤，直接将其拼接进了 SQL 查询语句中，导致系统出现 SQL 注入漏洞。

- **漏洞标签**

  涉及 HVV 重点系统、影响范围广、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  sql 注入

- **检测规则**

  106058039

- **受影响版本**

  - 用友 GRP-U8R10 U8Manager B、C、G 系列产品 < 20230905

- **修复建议**

  - 目前官方已发布更新补丁，建议获取版本升级安装包或补丁；

    官方下载链接：

    百度云盘：https://pan.baidu.com/s/1cQIxlUkpYAxE508EXjgQxA 提取码：n1xy

    用友云盘：https://pan.yonyou.com/s/gUWlv8QkSsY 密码：a61h

  - 下载【20230905-关于用友 GRP-U8 bx_historyDataCheck jsp 存在 SQL 注入漏洞的解决方案.zip】

  - 更新用友 GRP-U8 Manager 产品的 2023 年 10 月份（日期大于等于均可）标准补丁也可以修复此问题。

2.39 用友 U8 Cloud /ServiceDispatcherServlet 反序列化漏洞

- **漏洞描述**

  用友 U8Cloud 是一款企业级 ERP，用于协助企业实现业务协同和流程管理

的高效化和数字化。

未经身份验证的远程攻击者通过 ServiceDispatcher 接口发送恶意数据包，利用反序列化数据包，成功利用该漏洞可以命令执行，导致系统被攻击与控制。

- **漏洞标签**

  涉及 HVV 重点系统、影响范围广、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  反序列化，代码执行

- **检测规则**

  106053618

- **受影响版本**

  - U8Cloud 所有版本

- **修复建议**

  - 官方已发布升级补丁包，可在官方公告中进行下载安装；
  - 官方下载链接：https://security.yonyou.com/#/patchInfo?foreignKey=7bd5b43e2c984a618b2b1d3f288110ae
  - 建议客户部署 WAF、RASP 等工具，同时应避免用友 U8Cloud 系统暴露在公网。

2.40 JumpServer 堡垒机 会话回放未授权访问漏洞

- **漏洞描述**

JumpServer 是一款开源的堡垒机。

在 JumpServer 受影响版本中，由于会话回放录像接口 /api/v1/terminal/sessions/鉴权不当，未授权的攻击者可以通过直接访问 /api/v1/terminal/sessions/接口查看并下载会话回放录像数据。当会话回放存储在 S3 或 OSS 或其他云存储中，则不受此漏洞影响。

- **漏洞标签**

  国产开源框架、影响范围广、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  CVE-2023-42442

- **漏洞类型**

  权限绕过，信息泄露

- **检测规则**

  106057904

- **受影响版本**

  - JumpServer v3.0.0-v3.5.4
  - JumpServer v3.6.0-v3.6.3

- **修复建议**

  - 目前，JumpServer 官方已发布漏洞修复补丁，建议受影响用户升级至：

    JumpServer v3.5.5

    JumpServer >= v3.6.4

  - 官方下载链接：https://www.fit2cloud.com/jumpserver/index.html

2.41 致远 OA 前台任意用户密码重置漏洞

- **漏洞描述**

  致远 A8+协同管理平台，主要面向中大型、集团型企业和组织的协同管理软件产品。产品聚焦企业"智慧流程、业务定制、统一门户、移动办公、应用集成、数字决策"六大核心需求，同时具备智能化、平台化、移动化、定制化、数字化五大特性。

  致远 OA 存在短信验证码绕过重置密码漏洞，未经授权的远程攻击者在已知用户名的情况下可通过发送 HTTP 请求来触发任意用户密码重置，最终可导致任意用户登录。

- **漏洞标签**

  服务器权限、影响范围广、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  权限绕过

- **检测规则**

  106053616

- **受影响版本**

  - 致远 OA V5/G6 V8.1SP2、V8.2 版本

- **修复建议**

  - 官方已发布升级补丁包，可在官方公告中进行下载安装补丁 230810-S014；
  - 官方下载链接：https://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=171

2.42 iDocView /html/2word 远程代码执行漏洞

- **漏洞描述**

  iDocView 在线文档预览系统是由北京卓软在线信息技术有限公司开发的一套系统，可以上传本地文档预览，也可以直接预览网络文档、服务器磁盘路径文档、共享路径文档、FTP 文档等。

  该产品存在安全漏洞，攻击者把存在命令执行的 jsp 脚本放到 docview 目录下，利用特殊的方式访问该 jsp 脚本，可以导致远程代码执行。

- **漏洞标签**

  服务器权限、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  103045358

- **受影响版本**

  - iDocView < 13.10.1_20231115

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网获取版本升级安装包或补丁；
  - 官方下载链接：https://www.idocv.com/about.html

2.43 JeecgBoot 积木报表 testConnection JDBC 远程代码执行

- **漏洞描述**

  Jeecg (J2EE C ode G eneration)是一款基于代码生成器的低代码开发平台，使用 JEECG 可以简单快速地开发出企业级的 Web 应用系统。目前官方已停止维护。积木报表积木报表是其中的低代码报表组件。

  jeecg-boot/jmreport/testConnection Api 接口未进行身份验证，并且未对 dbUrl 参数进行限制，导致攻击者可以向指定地址发起 JDBC 请求。

- **漏洞标签**

  服务器权限、国产开源框架 、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行，反序列化

- **检测规则**

  106053872

- **受影响版本**

  - 3.0<JeecgBoot<3.5.3

- **修复建议**

- 官方已停止维护，建议利用安全组设置其仅对可信地址开放。

2.44 大华 DSS 综合管理平台 /portal/attachment_downloadByUrlAtt.action 路径存在任意文件下载漏洞

➢ 漏洞描述

大华 DSS（Digital Surveillance System）综合管理平台是大华技术有限公司（Dahua Technology）推出的一种视频监控管理软件。它是一套集视频监控、报警管理、智能分析、远程监控和数据管理等功能于一体的综合管理平台。

大华城市安防监控系统平台管理存在任意文件下载漏洞，黑客可以利用该漏洞下载任意文件，严重泄露计算机信息。

➢ 漏洞标签

工具/武器化成熟、影响范围广、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

任意文件读取

➢ 检测规则

103020821

➢ 受影响版本

暂无

➢ 修复建议

- 特殊字符过滤：检查用户输入，过滤或转义含有“…/”、“…\”、“%00”，“…”，“./”，“#”等跳转目录或字符终止符、截断字符的输入；
- 合法性判断：严格过滤用户输入字符的合法性，比如文件类型、文件地址、文件内容等；
- 白名单：白名单限定访问文件的路径、名称及后缀名；

- 提供设备的型号、序列号、项目名称、项目所在地、对应区域接口人、设备当前版本及发布日期、客户邮箱号码寻求厂商支持。

2.45 大华智慧园区综合管理平台 /user_getUserInfoByUserName.action 未授权任意用户密码读取

➢ 漏洞描述

大华智慧园区综合管理平台是一款综合管理平台，具备园区运营、资源调配和智能服务等功能。平台意在协助优化园区资源分配，满足多元化的管理需求，同时通过提供智能服务，增强使用体验。

由于该平台未对接口权限做限制，攻击者可以从 user_getUserInfoByUserName.action 接口获取任意用户密码(MD5 格式)。

➢ 漏洞标签

影响范围广、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

CNNVD-2023-03461037

➢ 漏洞类型

信息泄露

➢ 检测规则

106047793

➢ 受影响版本

- 大华智慧园区综合管理平台目前所有版本

➢ 修复建议

- 目前，官方已发布新版本，建议访问官网获取最新版本或补丁；
- 官方下载链接：https://www.dahuatech.com/cases/info/76.html

2.46 红帆 OA zyy_AttFile.asmx SQL 注入漏洞

- **漏洞描述**

  红帆 iOffice.net 从最早满足医院行政办公需求（传统 OA），到目前融合了卫生主管部门的管理规范和众多行业特色应用，是目前唯一定位于解决医院综合业务管理的软件，是最符合医院行业特点的医院综合业务管理平台，是成功案例最多的医院综合业务管理软件。

  红帆 JOffice. net zyy_AttFile.asmx 接口处存在 SQL 注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  106055812

- **受影响版本**

  暂无

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网获取最新版本或补丁；
  - 官方下载链接：https://www.ioffice.cn/wzsy

2.47 深信服数据中心管理系统 /src/sangforindex XML 实体注入漏洞

- **漏洞描述**

  深信服数据中心管理系统 DC 为 AC 的外置数据中心，主要用于海量日志

数据的异地扩展备份管理，多条件组合的高效查询，统计和趋势报表生成，设备运行状态监控等功能。

深信服数据中心管理系统 DC 存在 XML 外部实体注入漏洞。由于后端对传入的 XML 对象进行了非预期内解析，攻击者可以利用该漏洞进行 XML 注入攻击，获取系统敏感信息。

- **漏洞标签**

  影响范围广 、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106047925

- **受影响版本**

  - SANGFOR 数据中心<=v6.1

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网升级至 v11.0 及以上版本；
  - 官方下载链接：https://www.sangfor.com.cn/

2.48 大华智慧园区综合管理平台 /publishing/publishing/material/file/video 存在任意文件上传

- **漏洞描述**

  大华智慧园区综合管理平台是一款综合管理平台，具备园区运营、资源调配和智能服务等功能。平台意在协助优化园区资源分配，满足多元化的管理需求，同时通过提供智能服务，增强使用体验。

  大华智慧园区设备开放了文件上传功能，但未在上传的文件类型、大小、格式、路径等方面进行严格的限制和过滤，导致攻击者可以通过构造恶意

文件并上传到设备上，然后利用该漏洞获取权限并执行任意命令。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  文件上传

- **检测规则**

  103045563

- **受影响版本**

  - 大华智慧园区综合管理平台目前所有版本。

- **修复建议**

  - 建议使用相关系统的用户在尽快打补丁的同时，做好访问来源的限制，尽量避免大华智慧园区综合管理平台暴露在公网或不安全的网络环境中。

2.49 用友 TurboCRM /ajax/getemaildata.php 任意文件下载漏洞

- **漏洞描述**

  用友 U8 CRM 客户关系管理系统是一款专业的企业级 CRM 软件，旨在帮助企业高效管理客户关系、提升销售业绩和提供优质的客户服务。

  用友 U8 CRM 客户关系管理系统 getemaildata. php 文件存在任意文件上传和任意文件读取漏洞，攻击者通过漏洞可以获取到服务器权限。

- **漏洞标签**

  服务器权限、影响范围广、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  任意文件读取

- **检测规则**

  106047247

- **受影响版本**

  - 用友 U8 CRM <= V12.1

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：http://www.yonyou.com/

2.50 用友时空 KSOA 软件 /servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet SQL 注入漏洞

- **漏洞描述**

  用友时空 KSOA 是建立在 SOA 理念指导下研发的新一代产品，是根据流通企业最前沿的 IT 需求推出的统一的 IT 基础架构，它可以让流通企业各个时期建立的 IT 系统之间彼此轻松对话，帮助流通企业保护原有的 IT 投资，简化 IT 管理，提升竞争能力，确保企业整体的战略目标以及创新活动的实现。

  用友时空 KSOA /servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet 接口和/servlet/imagefield 接口处存在 SQL 注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷。

- **漏洞标签**

  服务器权限、国产开源框架、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

SQL 注入

- **检测规则**

  106054189

- **受影响版本**

  - 用友时空 KSOA v9.0

- **修复建议**

  - 厂商已提供漏洞修复方案。
  - 官方下载链接：http://www.yonyou.com/

2.51 金蝶云星空 /CommonFileServer 存在任意文件读取漏洞

- **漏洞描述**

  金蝶云星空是金蝶软件推出的一款云计算平台，旨在为企业提供全面的云服务和解决方案。它将金蝶软件丰富的企业管理应用和云计算技术相结合，帮助企业实现数字化转型和业务的快速发展

  金蝶云星空 V7.X、V8.X 所有私有云和混合云版本存在一个通用漏洞，攻击者可利用此漏洞获取服务器上的任意文件，包括数据库凭据、API 密钥、配置文件等，从而获取系统权限和敏感信息。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  任意文件读取

- **检测规则**

  106047697

- **受影响版本**

- 金蝶云星空企业版私有云、企业版私有云（订阅）、标准版私有云（订阅）三个产品
- 涉及版本：V6.2（含 17 年 12 月补丁）至 V8.1（含 23 年 9 月补丁）

➢ **修复建议**

- 目前官方已经发布补丁，建议受影响用户尽快安装补丁；
- 官方下载链接：https://vip.kingdee.com/school/detail/505412093244235264?productLineId=1
- 若客户暂时无法升级，应避免将受影响系统对公可访问，可通过设置网络 ACL 策略限制访问来源，例如只允许特定 IP 地址或地址段的访问。

2.52 大华智慧园区综合管理平台 /portal/services/carQuery/getFaceCapture/searchJson 存在 SQL 注入

➢ **漏洞描述**

大华智慧园区综合管理平台是一款综合管理平台，具备园区运营、资源调配和智能服务等功能。平台意在协助优化园区资源分配，满足多元化的管理需求，同时通过提供智能服务，增强使用体验。

由于该平台未对用户输入数据做限制，攻击者可以直接将恶意代码拼接进 SQL 查询语句中，导致系统出现 SQL 注入漏洞。

➢ **漏洞标签**

工具/武器化成熟、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

➢ **漏洞编号**

暂无

➢ **漏洞类型**

SQL 注入

➢ **检测规则**

103045564

➢ **受影响版本**

- 大华智慧园区综合管理平台目前所有版本

➢ 修复建议

- 建议使用相关系统的用户在尽快打补丁的同时，做好访问来源的限制，尽量避免大华智慧园区综合管理平台暴露在公网或不安全的网络环境中。

2.53 企业微信 /cgi-bin/gateway/agentinfo 接口存在未授权访问

➢ 漏洞描述

企业微信是腾讯微信团队为企业打造的专业办公管理工具。与微信一致的沟通体验,丰富免费的 OA 应用,并与微信消息、小程序、微信支付等互通,助力企业高效办公和管理。

2023 年 8 月，互联网上披露其相关接口存在未授权访问漏洞，在私有部署情况下，攻击者可构造恶意请求（/cgi-bin/gateway/agentinfo）获取企业微信 secret 等敏感信息，并组合调用相关 API 接口。

➢ 漏洞标签

影响范围广、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

权限绕过，信息泄露

➢ 检测规则

103045579

➢ 受影响版本

- 企业微信 2.5.x 版本
- 企业微信 2.6.930000 版本以下

➢ 修复建议

- 目前，官方已发布新版本，建议访问官网升级至新版本；

- 官方下载链接：

  https://link.zhihu.com/?target=https%3A//developer.work.weixin.qq.com/document/path/91039

2.54 绿盟安全审计系统 SAS /api/virtual/home/status 任意用户登录漏洞

➢ 漏洞描述

绿盟安全审计系统（Security Audit System，简称 SAS）是绿盟科技推出的一套企业级网络安全审计解决方案。它通过对网络设备、服务器和应用系统的日志进行全面收集、分析和审计，帮助企业实现对网络安全事件和风险的监控和管理。

绿盟安全审计系统 SAS local user.php 接口处存在权限绕过漏洞，未经身份验证的攻击者可以访问他们通常无权访问的敏感资源，最终导致系统处于极度不安全状态。

➢ 漏洞标签

影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

权限绕过

➢ 检测规则

106047726

➢ 受影响版本

暂无

➢ 修复建议

- 厂商已提供漏洞修复方案；
- 官方下载链接：
  https://www.nsfocus.com.cn/html/2019/197_0926/19.html

2.55 Jeecg-Boot Freemarker /jmreport/queryFieldBySql 模版注入漏洞

- **漏洞描述**

  Jeecg (J2EE C ode G eneration)是一款基于代码生成器的低代码开发平台，使用 JEECG 可以简单快速地开发出企业级的 Web 应用系统。目前官方已停止维护。

  jeect-boot 积木报表由于未授权的 API /jmreport/queryFieldBySql 使用了 freemarker 解析 SQL 语句从而导致了 RCE 漏洞的产生。

- **漏洞标签**

  漏洞编号服务器权限、国产开源框架 、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106047805

- **受影响版本**

  - JimuReport < 1.6.1

- **修复建议**

  - 官方已停止维护，建议利用安全组设置其仅对可信地址开放。

2.56 亿赛通电子文档安全管理系统 /UploadFileFromClientServiceForClient 任意文件上传漏洞

- **漏洞描述**

  亿赛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。

亿赛通电子文档安全管理系统 UploadFileFromClientServiceForClient 接口处存在任意文件上传漏洞，未经授权的攻击者可通过此漏洞上传恶意后门文件，从而获取服务器权限。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  文件上传

- **检测规则**

  106053305

- **受影响版本**

  - 目前所有版本

- **修复建议**

  - 应避免将受影响系统对公可访问，可通过设置网络 ACL 策略限制访问来源，例如只允许特定 IP 地址或地址段的访问。

2.57 用友时空 KSOA 软件 /servlet/imagefield SQL 注入漏洞

- **漏洞描述**

  用友时空 KSOA 是建立在 SOA 理念指导下研发的新一代产品，是根据流通企业最前沿的 IT 需求推出的统一的 IT 基础架构，它可以让流通企业各个时期建立的 IT 系统之间彼此轻松对话，帮助流通企业保护原有的 IT 投

资，简化 IT 管理，提升竞争能力，确保企业整体的战略目标以及创新活动的实现。

用友时空 KSOA /servlet/imagefield 接口处存在 SQL 注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷。

- **漏洞标签**

服务器权限、国产开源框架、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

SQL 注入

- **检测规则**

103045275

- **受影响版本**

  - 用友时空 KSOA v9.0

- **修复建议**

  - 厂商已提供漏洞修复方案；
  - 官方下载链接：http://www.yonyou.com/

2.58 用友-移动系统管理平台 uploadApk.do 任意文件上传漏洞

- **漏洞描述**

用友移动系统管理是用友公司推出的一款移动办公解决方案，旨在帮助企业实现移动办公、提高管理效率和员工工作灵活性。它提供了一系列功能和工具，方便用户在移动设备上管理和处理企业的系统和业务。

用友移动管理系统 uploadApk.do 接口存在任意文件上传漏洞，未经授权攻击者通过漏洞上传任意文件，最终可以获取服务器权限。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大 、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  文件上传

- **检测规则**

  106054194

- **受影响版本**

  暂无

- **修复建议**

  - 关闭无用服务；
  - 关注官方补丁更新，官方下载链接：http://www.yonyou.com/

2.59 泛微 E-Office v9 /E-mobile/App/Init.php 文件包含漏洞

- **漏洞描述**

  泛微 E-Office9 是一款企业级办公自动化系统，主要用于优化和管理企业的文档、信息流转、协作与沟通工作流程。

  泛微 E-Office 协同办公平台/E-mobile/App/Init.php 接口存在 SQL 注入漏洞，攻击者可利用该漏洞执行任意 SQL 语句，进行增、删、改、查等数据库操作，造成数据库敏感数据信息泄露或被篡改。

- **漏洞标签**

  影响范围广、漏洞价值大、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

代码执行

- **检测规则**

  103045567

- **受影响版本**

  - E-office9

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网获取版本升级安装包或补丁；
  - 官方下载链接：https://www.e-office.cn/

2.60 泛微 OA ifNewsCheckOutByCurrentUser SQL 注入漏洞

- **漏洞描述**

  泛微 E-cology 的 ifNewsCheckOutByCurrentUser.dwr 文件存在 SQL 注入漏洞。

- **漏洞标签**

  影响范围广 、漏洞价值大、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  106047764

- **受影响版本**

  暂无公开

- **修复建议**

  - 目前，官方已发布新版本，建议访问官网获取版本升级安装包或补丁；
  - 官方下载链接：https://www.weaver.com.cn/cs/securityDownload.asp

2.61 致远 OA syncConfigManager 方法存在远程代码执行漏洞

- **漏洞描述**

  远程攻击者在无需登录的情况下可通过向 URL /seeyon/htmlofficeservlet POST 精心构造的数据即可向目标服务器写入任意文件，写入成功后可执行任意系统命令进而控制目标服务器。

- **漏洞标签**

  服务器权限、影响范围广、漏洞价值大、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106054214

- **受影响版本**

  - 致远 A8-V5 协同管理软件 V6.1sp1
  - 致远 A8+协同管理软件 V7.0、V7.0sp1、V7.0sp2、V7.0sp3
  - 致远 A8+协同管理软件 V7.1

- **修复建议**

  - 对路径 /seeyon/htmlofficeservlet 进行限制访问。

2.62 深信服应用交付系统 /rep/login 远程命令执行漏洞

- **漏洞描述**

  深信服应用交付管理系统 login 存在远程命令执行漏洞，攻击者通过漏洞可以获取服务器权限，执行任意命令

- **漏洞标签**

  服务器权限、漏洞价值大、软件供应链风险、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106054566

- **受影响版本**

  - 深信服 应用交付管理系统 7.0.8-7.0.8R5

- **修复建议**

  - 关注官方信息：

    https://www.sangfor.com.cn/product-and-solution/sangfor-cloud/ad
    https://blog.csdn.net/nnn2188185/article/details/133365748

2.63 汉得 SRM tomcat.jsp 登陆绕过漏洞

- **漏洞描述**

  汉得 SRM tomcat.jsp 文件存在登陆绕过漏洞，攻击者通过发送请求包，可以获取后台管理员权限

- **漏洞标签**

  服务器权限、漏洞价值大、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  权限绕过

- **检测规则**

106047706

- **受影响版本**

  暂无

- **修复建议**

  - 限制对路径/tomcat.jsp?dataName=role_id&dataValue=1 的访问；
  - 限制对路径/tomcat.jsp?dataName=user_id&dataValue=1 的访问。

2.64 华天动力 OA /workFlowService 接口存在 SQL 注入漏洞

- **漏洞描述**

  华天动力 OA 8000 版 workFlowService 接口存在 SQL 注入漏洞，攻击者通过漏洞可获取数据库敏感信息

- **漏洞标签**

  影响范围广、漏洞价值大、红队打点必备

- **漏洞编号**

  CNVD-2021-46917

- **漏洞类型**

  SQL 注入

- **检测规则**

  106052919

- **受影响版本**

  暂无

- **修复建议**

  - 厂商尚未提供漏洞修复方案，请关注厂商主页更新：
    http://www.oa8000.com/

2.65 辰信领创辰信景云终端安全管理系统 /api/user/login

SQL 注入漏洞

- **漏洞描述**

辰信景云终端安全管理系统 login 存在 SQL 注入漏洞，攻击者通过漏洞可以获取数据库敏感信息。

- **漏洞标签**

影响范围广、漏洞价值大、红队打点必备

- **漏洞编号**

暂无

- **漏洞类型**

SQL 注入

- **检测规则**

103045210

- **受影响版本**

暂无

- **修复建议**

  - 对数据库进行严格监控；
  - 对用户提交数据信息严格把关，多次筛选过滤；
  - 用户内数据内容进行加密；
  - 升级至最新版本，设置其仅对可信地址开放。

2.66 安恒明御堡垒机 /service/ 任意用户注册漏洞

- **漏洞描述**

安恒明御堡垒机 /service/接口存在漏洞，攻击者通过漏洞可以添加任意用户控制堡垒机。

- **漏洞标签**

服务器权限、影响范围广、漏洞价值大、涉及 HVV 重点系统

- **漏洞编号**

暂无

- **漏洞类型**

  权限绕过

- **检测规则**

  106054187

- **受影响版本**

  暂无

- **修复建议**

  - 对新注册用户的绑定手机号进行身份认证；
  - 建议联系软件厂商进行处理。

2.67 绿盟 SAS 堡垒机 /webconf/Exec 远程代码执行漏洞

- **漏洞描述**

  绿盟 SAS 堡垒机 Exec 远程命令执行漏洞。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  103045562

- **受影响版本**

  - 绿盟安全审计系统 SAS V5.6R10F00*
  - 绿盟安全审计系统 SAS V5.6R10F01*
  - 绿盟安全审计系统 SAS V5.6R10F02*-V5.6R10F05*

- **修复建议**
  - V5.6R10F00*版本建议升级到 V5.6R10F00SP21 版本；
  - V5.6R10F01*版本建议升级到 V5.6R10F01SP08 版本；
  - V5.6R10F02*-V5.6R10F05*版本建议升级到 V5.6R10F05SP04 版本；
  - 升级包获取链接如下：https://update.nsfocus.com/update/listSash。

2.68 绿盟 SAS 堡垒机 /webconf/GetFile 任意文件读取漏洞

- **漏洞描述**

  绿盟安全审计系统-堡垒机系列 提供一套先进的运维安全管控与审计解决方案，绿盟堡垒机 GetFile 方法存在任意文件读取漏洞，攻击者通过漏洞可以读取服务器中的任意文件。

- **漏洞标签**

  影响范围广、漏洞价值大 、红队打点必备、涉及 HVV 重点系统

- **漏洞编号**

  暂无

- **漏洞类型**

  任意文件读取

- **检测规则**

  103045209

- **受影响版本**
  - 绿盟安全审计系统 SAS V5.6R10F00*
  - 绿盟安全审计系统 SAS V5.6R10F01*
  - 绿盟安全审计系统 SAS V5.6R10F02*-V5.6R10F05*

- **修复建议**
  - V5.6R10F00*版本建议升级到 V5.6R10F00SP21 版本；
  - V5.6R10F01*版本建议升级到 V5.6R10F01SP08 版本；

- V5.6R10F02*-V5.6R10F05*版本建议升级到 V5.6R10F05SP04 版本；
- 升级包获取链接如下：https://update.nsfocus.com/update/listSash。

2.69 广联达 OA GetIMDictionary 接口存在 SQL 注入漏洞

➢ 漏洞描述

由于广联达 Linkworks 办公 OA GetIMDictionary 接口未对用户的输入进行有效过滤，将其拼接进了 SQL 查询语句中，导致系统出现 SQL 注入漏洞。而 msgbroadcastuploadfile.aspx 接口处存在后台文件上传漏洞，攻击者通过 SQL 注入获取管理员信息后，可以登录发送请求包获取服务器权限。

➢ 漏洞标签

服务器权限、影响范围广、漏洞价值大、红队打点必备

➢ 漏洞编号

暂无

➢ 漏洞类型

SQL 注入

➢ 检测规则

103045212

➢ 受影响版本

暂无

➢ 修复建议

- 限制访问来源地址，如非必要，不要将系统开放在互联网上；
- 更新至最新版本。

2.70 Smartbi setEngineAddress 权限绕过漏洞

➢ 漏洞描述

Smartbi 大数据分析平台存在远程命令执行漏洞，未经身份认证的远程攻击者可利用 stub 接口构造请求绕过补丁限制，进而控制 JDBC URL，最终可导

致远程代码执行或信息泄露。

- **漏洞标签**

  影响范围广、工具/武器化成熟、红队打点必备

- **漏洞编号**

  暂无

- **漏洞类型**

  权限绕过

- **检测规则**

  106054181

- **受影响版本**

  - v7 <= Smartbi <= v10.5.8

- **修复建议**

  - 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

2.71 WPS Office 客户端远程代码执行漏洞

- **漏洞描述**

  WPS Office for Windows 目前侦测到处理某种 OLD (Object Lin king and Embedding ，中文名为”对象链接与嵌入”)时存在逻辑漏洞，攻击者可以利用该漏洞专门制造出恶意的 pps 或 ppsx 格式档案（一种开启即投影播放的演示文件格式），如果用户开启该文件在播放时鼠标移动或点击 OLE 区域，则会连网从远程服务器下载恶意代码并执行，此时会下载后门程序并投放在系统启动目录，攻击者进而在用户重启计算机时控制用户计算机。

- **漏洞标签**

  影响范围广、工具/武器化成熟、国产办公系统

- **漏洞编号**

  暂无

- **漏洞类型**

代码执行

- **检测规则**

  103044100

- **受影响版本**

  - WPS Office for Windows 个人版 版号低于 11.1.0.12116（含）
  - WPS Office for Windows 企业版 版号低于 11.8.2.11707（含）

- **修复建议**

  - 把 WPS 升级到最新版本；
  - 官方已发布相关补丁，如果您在使用 WPS office 的企业版请尽快联系官方技术工程师或客服获取最新版本，并确保企业版升级到 11.8.2.12085;如果您使用的是 WPS ffice 个人版，请通过 WPS 官网 https: //www.wps.cn 获取最新版本进行升级。

2.72 海康威视-综合安防管理平台 /center/api/files 任意文件上传漏洞

- **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。

- **漏洞标签**

  影响范围广、工具/武器化成熟、国产系统

- **漏洞编号**

  CNVD-2022-88855

- **漏洞类型**

  代码执行

- **检测规则**

  106047644

- **受影响版本**
  - iVMS-8700 V2.0.0 - V2.9.2
  - iSecure Center V1.0.0 - V1.7.0
- **修复建议**
  - 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/
  - 临时禁用上传接口；
  - 对接口进行鉴权；
  - 系统采用白名单校验。

2.73 泛微 OA clusterupgrade 前台文件上传漏洞

- **漏洞描述**

  泛微 OA 10.58.3 补丁以下的版本存在前台文件上传漏洞，未经授权的远程攻击者可通过发送特殊的 HTTP 请求来触发文件上传，最终可导致攻击者获取远程服务器权限。
- **漏洞标签**

  工具/武器化成熟、红队打点必备、漏洞价值大
- **漏洞编号**

  暂无
- **漏洞类型**

  文件上传
- **检测规则**

  106013565
- **受影响版本**
  - 泛微 OA <10.58.3
- **修复建议**

- 官方已发布安全修复补丁，建议受影响的用户尽快升级至 v10.58.3 或之后的补丁版本。
- 下载地址：https://www.weaver.com.cn/cs/securityDownload.asp#

2.74 Metabase 远程代码执行漏洞

➢ 漏洞描述

Metabase 0.46.6.1 之前版本和 Metabase Enterprise 1.46.6.1 之前版本存在安全漏洞，该漏洞源于允许攻击者以服务器的权限级别在服务器上执行任意命令。

➢ 漏洞标签

影响范围广、工具/武器化成熟、服务器权限、红队打点必备、软件供应链风险、漏洞价值大

➢ 漏洞编号

CVE-2023-38646

➢ 漏洞类型

代码执行

➢ 检测规则

103045532

➢ 受影响版本

- Metabase:Metabase Community 0.46 < 0.46.6.1
- Metabase:Metabase Community 0.45 < v0.45.4.1
- Metabase:Metabase Community 0.44 < 0.44.7.1
- Metabase:Metabase Community 0.43 < 0.43.7.2
- Metabase:Metabase Enterprise 1.46 < 1.46.6.1
- Metabase:Metabase Enterprise 1.45 < 1.45.4.1
- Metabase:Metabase Enterprise 1.44 < 1,44.7.1
- Metabase:Metabase Enterprise 1.43 < 1.43.7.2

➢ 修复建议

- 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.metabase.com/blog/security-advisory

https://blog.assetnote.io/2023/07/22/pre-auth-rce-metabase/

2.75 奇安信 SSLVPN 存在未授权访问漏洞

- **漏洞描述**

  奇安信 vpn 存在未授权管理用户遍历及任意账号密码修改

- **漏洞标签**

  红队打点必备、漏洞价值大

- **漏洞编号**

  暂无

- **漏洞类型**

  信息泄露

- **检测规则**

  103020861

- **受影响版本**

  暂无

- **修复建议**

  暂无

2.76 Smartbi windowUnloading 未授权远程命令执行

- **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 URL 可以绕过登录校验代码，从而访问后台功能点。

- **漏洞标签**

  影响范围广、服务器权限、软件供应链风险、漏洞价值大

- **漏洞编号**

  暂无

- **漏洞类型**

  权限绕过

- **检测规则**

  106054181

- **受影响版本**

  - Smartbi >= V9

- **修复建议**

  - 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

2.77 泛微 OA E-Cology XXE 漏洞

- **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。

- **漏洞标签**

  影响范围广、工具/武器化成熟、国产系统

- **漏洞编号**

  暂无

- **漏洞类型**

  信息泄露

- **检测规则**

  106045809

- **受影响版本**

  - 泛微 e-cology9 补丁版本< 10.58

- **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：
  - 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

2.78 Smartbi 内置用户登陆绕过漏洞

- **漏洞描述**

  该漏洞源于 Smartbi 默认存在内置用户，在使用特定接口时，攻击者可绕过用户身份认证机制获取内置用户身份凭证，随后可使用获取的身份凭证调用后台接口，最终可能导致敏感信息泄露和代码执行。

- **漏洞标签**

  影响范围广、工具/武器化成熟、国产系统

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106047643

- **受影响版本**

  - V7 <= Smartbi <=V10

- **修复建议**

  - 官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，酌情升级至安全版本：

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

2.79 Alibaba Nacos Jraft 反序列化漏洞

- **漏洞描述**

  该漏洞源于 Nacos 集群处理部分 Jraft 请求时，未限制使用 hessian 进行反序列化，攻击者可以通过发送特制的请求触发该漏洞，最终执行任意远程代码。

- **漏洞标签**

  服务器权限、工具/武器化成熟、国产开源框架、影响范围广、漏洞价值大

- **漏洞编号**

  CNVD-2023-45001

- **漏洞类型**

  代码执行

- **检测规则**

  106047651

- **受影响版本**

  - 1.4.0 <= Nacos < 1.4.6
  - 2.0.0 <= Nacos < 2.2.3

- **修复建议**

  - 默认配置下该漏洞仅影响 Nacos 集群间 Raft 协议通信的 7848 端口，此端口不承载客户端请求，可以通过限制集群外部 IP 访问 7848 端口来进行缓解；
    - 官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，酌情升级至安全版本：https://github.com/alibaba/nacos/releases

2.80 瑞友天翼应用虚拟化系统 GetBSAppUrl SQL 注入漏洞

- **漏洞描述**

  瑞友天翼应用虚拟化系统是基于服务器计算架构的应用虚拟化平台，它将

用户各种应用软件集中部署到瑞友天翼服务集群，客户端通过 WEB 即可访问经服务器上授权的应用软件，实现集中应用、远程接入、协同办公等。未经身份认证的远程攻击者可以利用系统中存在的 SQL 注入漏洞，写入后门文件，从而执行远程代码。

- **漏洞标签**

  涉及 HVV 重点系统、服务器权限、工具/武器化成熟

- **漏洞编号**

  暂无

- **漏洞类型**

  SQL 注入

- **检测规则**

  103045527

- **受影响版本**

  - 5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.3.1

- **修复建议**

  - 避免将该系统开放至公网；
  - 官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，建议您在升级前做好数据备份工作，避免出现意外，酌情升级至安全版本：http://soft.realor.cn:88/Gwt7.0.4.1.exe

2.81 nacos token.secret.key 身份认证绕过漏洞

- **漏洞描述**

  目前 Nacos 身份认证绕过漏洞(QVD-2023-6271)，开源服务管理平台 Nacos 在默认配置下未对 token.secret.key 进行修改，导致远程攻击者可以绕过密钥认证进入后台，造成系统受控等后果。

- **漏洞标签**

  利用条件简单、、工具/武器化成熟、服务器权限、红队打点必备、漏洞价值大

- **漏洞编号**

  QVD-2023-6271

- **漏洞类型**

  权限绕过

- **检测规则**

  106047602

- **受影响版本**

  - 0.1.0 <= Nacos <= 2.2.0

- **修复建议**

  - 升级至最新版本；
  - 修改默认密钥。

2.82 Weblogic 远程代码执行漏洞

- **漏洞描述**

  由于 Weblogic T3/IIOP 协议支持远程对象通过 bind 方法绑定到服务端，并且可以通过 lookup 方法查看，当远程对象继承自 OpaqueReference 类，使用 lookup 方法查看远程对象时，服务端会调用远程对象的 getReferent 方法。weblogic.deployment.jms.ForeignOpaqueReference 继承自 OpaqueReference 类，同时实现了 getReferent 方法，并且存在 retVal = context.lookup(this.remoteJNDIName)实现，故可以通过 rmi/ldap 远程协议进行远程命令执行。

- **漏洞标签**

  影响范围广、工具/武器化成熟、服务器权限、红队打点必备、软件供应链风险、漏洞价值大

- **漏洞编号**

  CVE-2023-21839

- **漏洞类型**

  代码执行，反序列化

- **检测规则**

  103044266

- **受影响版本**

- Oracle WebLogic Server 12.2.1.3.0
- Oracle WebLogic Server 12.2.1.4.0
- Oracle WebLogic Server 14.1.1.0.0

➢ **修复建议**

- 如不依赖 T3 协议进行通信，可通过阻断 T3 协议和关闭 IIOP 协议端口防止漏洞攻击，方法如下：
- 禁用 T3 协议：进入 Weblogic 控制台，在 base_domain 配置页面中，进入“安全”选项卡页面，点击“筛选器”，配置筛选器，然后在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则框中输入：* * 7001 deny t3 t3s；
- 关闭 IIOP 协议端口：在 WebLogic 控制台中，选择“服务”->”AdminServer”->”协议”，取消“启用 IIOP”的勾选，并重启 WebLogic 项目，使配置生效。官方已发布漏洞补丁及修复版本，可以评估业务是否受影响后，酌情升级至安全版本。

2.83 Microsoft Outlook 特权提升漏洞

➢ **漏洞描述**

该漏洞存在于 Microsoft Outlook 中，是一个身份验证绕过漏洞。未经身份验证的远程攻击者仅通过向受影响的系统发送特制电子邮件，从而访问用户的 Net-NTLMv2 哈希，进而可以在中继攻击中使用此哈希来冒充用户，从而有效地绕过身份验证。

➢ **漏洞标签**

利用条件简单、漏洞细节公开、红队打点必备

➢ **漏洞编号**

CVE-2023-23397

➢ **漏洞类型**

代码执行

➢ **检测规则**

103044288

➢ **受影响版本**

- 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

➢ 修复建议

- 目前微软官方已针对受支持的产品版本发布了修复该漏洞的安全补丁，建议受影响用户开启系统自动更新安装补丁进行防护。

  注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。右键点击 Windows 徽标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

- 针对未成功安装更新补丁的情况，可直接下载离线安装包进行更新，链接如下：

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

- 临时防护措施

  若用户无法正常进行补丁修复，在不影响正常业务的情况下，可使用以下措施对漏洞进行防护：

  将用户添加到受保护的用户安全组，以防止使用 NTLM 作为身份验证机制；

  注意：该操作可能会对需要 NTLM 的应用程序造成一定影响。

- 详情请参考：

  https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

- 用户可通过在网络中同时使用外围防火墙和本地防火墙，并通过 VPN 设置来阻止 TCP 445/SMB 从网络出站。

  注意：该操作将禁止发送 NTLM 身份验证消息到远程文件共享。

2.84 Apache Druid 远程代码执行漏洞

➢ 漏洞描述

该漏洞源于 Apache Kafka Connect JNDI 注入漏洞(CVE-2023-25194)，Apache Druid 由于支持从 Kafka 加载数据，刚好满足其利用条件，攻击者可通过修改 Kafka 连接配置属性进行 JNDI 注入攻击，进而在服务端执行任意恶意代码。

➢ 漏洞标签

服务器权限、数据库权限、涉及 HVV 重点系统

➢ 漏洞编号

暂无

➢ 漏洞类型

代码执行

➢ 检测规则

103045875

➢ 受影响版本

- Apache Druid <= 25.0.0

➢ 修复建议

- 避免 Apache Druid 开放至公网；
- 开启身份认证机制，可参考官方文档：https://druid.apache.org/docs/latest/development/extensions-core/druid-basic-security.html

2.85 Apache Solr 远程代码执行漏洞

➢ 漏洞描述

当 Solr 以 Solrcloud 模式启动且可出网时，未经身份验证的远程攻击者可以通过发送特制的数据包进行利用，最终在目标系统上远程执行任意代码。

- **漏洞标签**

  工具/武器化成熟、涉及 HVV 重点系统、服务器权限

- **漏洞编号**

  CNVD-2023-27598

- **漏洞类型**

  代码执行

- **检测规则**

  106047578

- **受影响版本**

  - 8.10.0 <= Apache Solr < 9.2.0

- **修复建议**

  - 如果未使用 ConfigSets API，请禁用 UPLOAD 命令，将系统属性：configset.upload.enabled 设置为 false，详细参考：

    https://lucene.apache.org/solr/guide/8_6/configsets-api.html

  - 使用身份验证/授权，详细参考：

    https://lucene.apache.org/solr/guide/8_6/authentication-and-authorization-plugins.html

  - 官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，酌情升级至安全版本：

    https://github.com/apache/solr/releases/tag/releases/solr/9.2.0

2.86 Grafana JWT 泄露漏洞

- **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。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞

- **漏洞编号**

  CVE-2023-1387

- **漏洞类型**

  权限绕过

- **检测规则**

  103045186

- **受影响版本**

  - 9.1.0 <= Grafana < 9.2.17
  - 9.3.0 <= Grafana < 9.3.13
  - 9.4.0 <= Grafana < 9.5.0

- **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：

    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

2.87 GitLab 远程代码执行漏洞

- **漏洞描述**

  恶意攻击者可以通过上传特殊构造的恶意项目，导致系统远程代码执行。

- **漏洞标签**

  工具/武器化成熟、服务器权限、漏洞价值大

- **漏洞编号**

  CVE-2022-2185

- **漏洞类型**

  代码执行

- **检测规则**

  106052631

- **受影响版本**

  - GitLab CE/EE 14.0 版本 < 14.10.5
  - GitLab CE/EE 15.0 版本 < 15.0.4
  - GitLab CE/EE 15.1 版本 < 15.1.1

- **修复建议**

  - 升级至最新版本，官方下载链接：https://about.gitlab.com/update/

2.88 F5 BIG-IP 命令执行漏洞

- **漏洞描述**

  F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。 F5 BIG-IP 存在访问控制错误漏洞，攻击者可以通过未公开的请求利用该漏洞绕过 BIG-IP 中的 iControl REST 身份验证来控制受影响的系统。

- **漏洞标签**

  影响范围广、历史重大漏洞、工具/武器化成熟

- **漏洞编号**

  CVE-2022-1388

- **漏洞类型**

  命令执行、身份认证缺陷

- **检测规则**

  103045029

- **受影响版本**
  - 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
- **修复建议**
  - 建议升级至最新版本或可参考官方修复建议 Recommended Actions：https://support.f5.com/csp/article/K23605346
  - 在受影响的版本内可执行以下步骤以缓解攻击：
  - 通过自身 IP 地址阻止 iControl REST 访问；
  - 通过管理界面阻止 iControl REST 访问；
  - 修改 BIG-IP httpd 配置。

2.89 Linux DirtyPipe 权限提升漏洞

- **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。漏洞作者将此漏洞命名为“Dirty Pipe”。

- **漏洞标签**

  影响范围广、漏洞细节公开、涉及 HVV 重点系统、漏洞价值大、服务器权限

- **漏洞编号**

  CVE-2022-0847

- **漏洞类型**

  代码执行、权限提升

- **检测规则**

  106012315

- **受影响版本**

  - 5.8 <= Linux 内核版本 < 5.16.11 / 5.15.25 / 5.10.102

- **修复建议**

  - 更新升级 Linux 内核到以下安全版本：

    Linux 内核= 5.16.11

    Linux 内核= 5.15.25

    Linux 内核= 5.10.102

  - 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

    https://www.debian.org/security/2022/dsa-5092

2.90 Atlasssian Confluence OGNL 注入漏洞

- **漏洞描述**

  在 Atlassian Confluence Server and Data Center 上存在 OGNL 注入漏洞，恶意攻击者可以利用该漏洞发送特制请求从而在目标服务器上注入恶意 OGNL 表达式，造成远程执行代码并部署 WebShell 。

- **漏洞标签**

  涉及 HVV 重点系统、工具/武器化成熟、历史重大漏洞、利用条件简单

- **漏洞编号**

  CVE-2022-26134

- **漏洞类型**

  代码执行

- **检测规则**

  106054835

- **受影响版本**

  - 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

➢ 修复建议

- 升级 Atlassian Confluence Server and Data Center 至安全版本；

  临时缓解方案：https://packages.atlassian.com/maven-internal/opensymphony/xwork/1.0.3-atlassian-10/xwork-1.0.3-atlassian-10.jar

  下载官方发布的 xwork-1.0.3-atlassian-10.jar 替换 confluence/WEB-INF/lib/目录下原来的 xwork jar 文件，并重启 Confluence。

2.91 XXL-JOB Executor 未授权访问漏洞

➢ 漏洞描述

XXL-JOB 是一个分布式任务调度平台，其核心设计目标是开发迅速、学习简单、轻量级、易扩展。现已开放源代码并接入多家公司线上产品线，开箱即用。XXL-JOB 分为 admin 和 executor 两端，前者为后台管理页面，后者是任务执行的客户端。

➢ 漏洞标签

影响范围广、红队打点必备、漏洞价值大

➢ 漏洞编号

暂无

➢ 漏洞类型

代码执行，权限绕过

➢ 检测规则

106057845

- **受影响版本**
  - XXL-JOB <=2.2.0
- **修复建议**
  - 开启 XXL-JOB 自带的鉴权组件：官方文档中搜索“xxl.job.accessToken”，按照文档说明启用即可；
  - 端口防护：及时更换默认的执行器端口，不建议直接将默认的 9999 端口开放到公网；
  - 端口访问限制：通过配置安全组限制只允许指定 IP 才能访问执行器 9999 端。

2.92 蓝凌 OA datajson.js script 远程代码执行漏洞

- **漏洞描述**

  蓝凌 OA 存在任意文件写入漏洞，攻击者可以上传恶意文件
- **漏洞标签**

  历史重大漏洞、红队打点必备、服务器权限、漏洞价值大
- **漏洞编号**

  暂无
- **漏洞类型**

  代码执行
- **检测规则**

  103046064
- **受影响版本**

  全版本
- **修复建议**
  - 升级蓝凌 OA 系统至最新版本；
  - 官网下载最新安全补丁：https://www.landray.com.cn/

2.93 蓝凌 OA treexml.tmpl script 远程代码执行漏洞

- **漏洞描述**

蓝凌 OA treexml.tmpl 存在远程命令执行漏洞，攻击者通过发送特定的请求包可以获取服务器权限。

- **漏洞标签**

工具/武器化成熟、服务器权限、软件供应链风险

- **漏洞编号**

暂无

- **漏洞类型**

代码执行

- **检测规则**

106058203

- **受影响版本**

暂无

- **修复建议**

  - 升级蓝凌 OA 系统至最新版本；
  - 官网下载最新安全补丁：https://www.landray.com.cn/

2.94 用友 NC FileReceiveServlet 文件上传漏洞

- **漏洞描述**

用友 NC6.5 的 FileReceiveServlet 接口，存在任意文件上传漏洞。漏洞成因在于上传文件处未作类型限制，未经身份验证的攻击者可通过向目标系统发送特制数据包来利用此漏洞，成功利用此漏洞的远程攻击者可在目标系统上传任意文件执行命令。

- **漏洞标签**

影响范围广、历史重大漏洞、红队打点必备

- **漏洞编号**

暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106050636

- **受影响版本**

  - NC > 6.5

- **修复建议**

  - 目前，官方暂未发布补丁公告，建议使用该产品用户及时关注官方安全漏洞公告和补丁更新动态。

2.95 泛微云桥 e-BridgeSQL 注入漏洞

- **漏洞描述**

  泛微云桥多个版本存在多处 SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感信息。

- **漏洞标签**

  工具/武器化成熟、历史重大漏洞、漏洞价值大

- **漏洞编号**

  CNVD-2022-43246

- **漏洞类型**

  SQL 注入

- **检测规则**

  106047088

- **受影响版本**

  - 泛微云桥 v4.0
  - 泛微云桥 v9.0 141103
  - 泛微云桥 v9.5 20220113

- **修复建议**
  - 更新系统；
  - 变量做好过滤和检测。

2.96 Apache Commons 远程代码执行漏洞

- **漏洞描述**

  该漏洞源于 Apache Commons Configuration2 执行变量 interpolation 时，允许动态评估和扩展属性。interpolation 的标准格式是“${prefix:name}”，其中“prefix”用于定位执行interpolation 的 org.apache.commons.configuration2.interpol.Lookup 的实例。从 2.4 版到 2.7 版，默认的 Lookup 实例可能导致任意代码执行或远程连接服务器。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限

- **漏洞编号**

  CVE-2022-33980

- **漏洞类型**

  代码执行

- **检测规则**

  106052912

- **受影响版本**
  - 2.4 <= Apache Commons Configuration <=2.7
- **修复建议**
  - 官方已发布漏洞补丁及修复版本，酌情升级至安全版本，下载链接如下：https://commons.apache.org/proper/commons-configuration/changes-report.html

2.97 泛微 OA 存在命令执行漏洞

- **漏洞描述**

泛微 OA 存在 SQL 注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。

- **漏洞标签**

工具/武器化成熟、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

CNVD-2022-43843

- **漏洞类型**

SQL 注入

- **检测规则**

106047125

- **受影响版本**

  - 泛微 OA v8（补丁 7.11 之前）

- **修复建议**

  - 厂商已提供漏洞修复方案，请关注厂商主页更新：

    http://v10.e-office.cn/9safepack/%E6%B3%9B%E5%BE%AEe-office9.5%2020220525%E8%A1%A5%E4%B8%81%E7%A8%8B%E5%BA%8F.zip

2.98 通达 OA 代码执行漏洞

- **漏洞描述**

通达 OA 存在命令执行漏洞。攻击者可利用该漏洞获取服务器权限。

- **漏洞标签**

影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

暂无

- **漏洞类型**

  代码执行

- **检测规则**

  103020622

- **受影响版本**

  - 全版本

- **修复建议**

  - V11 版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.11.3.exe
  - 2017 版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.10.19.exe
  - 2016 版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.9.13.exe
  - 2015 版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.8.15.exe
  - 2013 增强版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.7.25.exe
  - 2013 版：
    http://cdndown.tongda2000.com/oa/security/2020_A1.6.20.exe

2.99 FastJson 代码执行漏洞

- **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。

- **漏洞标签**

  国产开源框架、红队打点必备、服务器权限、漏洞价值大、工具/武器化成熟

- **漏洞编号**

  CVE-2022-25845

- **漏洞类型**

  代码执行

- **检测规则**

  106057108

- **受影响版本**

  - Fastjson ≤ 1.2.80

- **修复建议**

  - 升级至版本 FastJson 1.2.83：

    https://github.com/alibaba/fastjson/releases/tag/1.2.83

  - 升级到 FastJosn v2：

    https://github.com/alibaba/fastjson2/releases

2.100 禅道存在 SQL 注入漏洞

- **漏洞描述**

  禅道存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

- **漏洞标签**

  影响范围广、工具/武器化成熟、红队打点必备

- **漏洞编号**

  CNVD-2022-42853

- **漏洞类型**

  SQL 注入

- **检测规则**

  103044176

- **受影响版本**

  - 禅道企业版 6.5

- 禅道旗舰版 3.0 8
- 禅道开源版 16.5
- 禅道开源版 16.5.beta1

➢ **修复建议**

- 厂商已提供漏洞修补方案，请关注厂商主页及时更新：
  https://www.zentao.net/

2. 101 ThinkPHP v5.x 远程代码执行漏洞

➢ **漏洞描述**

该漏洞是由于 ThinkPHP5 在处理控制器传参时，没有对参数进行充分的过滤与验证，导致恶意用户可以通过提交恶意数据，构造出一个带有 PHP 函数的控制器方法，并通过 URL 参数的形式访问该方法，从而触发远程代码执行漏洞。

➢ **漏洞标签**

影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

➢ **漏洞编号**

暂无

➢ **漏洞类型**

代码执行

➢ **检测规则**

103020752

➢ **受影响版本**

- thinkphp v5.x

➢ **修复建议**

- 官方已经发布了修复该漏洞的版本，建议用户及时升级到 5.0.23 或 5.1.30 版本。

2.102 明御 Web 应用防火墙任意登录

- **漏洞描述**

  代码/waf/php_admin/app/mvc/controllers/controller/report.php 中以硬编码形式设置了 console 用户登录， 通过下述代码可以直接登录。登录后台，构造了恶意的保护站点配置，覆盖了会调用 webapp.yaml，其中 ip 参数可进行命令注入。由此，构造出恶意的保护站点配置的加密数据包， 通过管理员用户登录后台，上传恶意数据包进行 RCE。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  暂无

- **漏洞类型**

  权限绕过

- **检测规则**

  106047523

- **受影响版本**

  - 明御 WAF X86 架构 <= 4.6.33
  - 明御 WAF 信创兆芯 = 4.5
  - 明御 WAF 鲲鹏 = 4.6.18

- **修复建议**

  - 限制 aaa_local_web_preview 的访问权限；
  - 建议联系软件厂商进行处理。

2.103 Laravel 存在命令执行漏洞

- **漏洞描述**

  Laravel 是一套 PHP Web 开发框架（PHP Web Framework）。Laravel 存在命令执行漏洞，攻击者可利用漏洞进行远程代码执行（RCE）。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  CNVD-2022-44351

- **漏洞类型**

  命令执行

- **检测规则**

  106047924

- **受影响版本**

  - Laravel 9.1.8

- **修复建议**

  - 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://laravel.com/

2.104 安恒 WEB 应用防火墙远程命令执行漏洞

- **漏洞描述**

  安恒明御 WEB 应用防火墙 report.php 文件存在硬编码设置的 Console 用户登录，攻击者可以通过漏洞直接登录后台。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  暂无

- **漏洞类型**

  命令执行

- **检测规则**

  106047927

- **受影响版本**
  - <= V3.0.4.6.33
- **修复建议**
  - 明御 WEB 应用防火墙 V3.0.4.6.33 及以下版本存在该漏洞，在 V3.0.4.6.34 此漏洞已完成修复，不影响产品自身安全。

2.105 QAX 天擎版本<6.7.0.4910 存在安全漏洞

- **漏洞描述**

  暂不公开
- **漏洞标签**

  影响范围广、漏洞价值大、软件供应链风险
- **漏洞编号**

  暂无
- **漏洞类型**

  代码执行
- **检测规则**

  103045045
- **受影响版本**
  - 奇安信天擎版本<6.7.0.4910
- **修复建议**
  - 版本升级到 6.7.0.4910 以上。

2.106 泛微 E-office SQL 注入漏洞

- **漏洞描述**

  泛微 E-office 的 json_common.php 接口存在 SQL 注入漏洞，未经身份验证的恶意攻击者利用此漏洞获取数据库中的信息。

- **漏洞标签**

  工具/武器化成熟、历史重大漏洞、红队打点必备

- **漏洞编号**

  CNVD-2022-43246

- **漏洞类型**

  SQL 注入

- **检测规则**

  106047088

- **受影响版本**

  - e-office <=9.5

- **修复建议**

  - 厂商已经发布修复补丁，请及时更新：https://www.e-office.cn/

2.107 Apache Log4j2 远程代码执行漏洞

- **漏洞描述**

  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。

  Apache Log4j2 存在远程代码执行漏洞，该漏洞是由于 Apache Log4j2 某些功能存在递归解析功能，未经身份验证的攻击者通过发送特定恶意数据包，可在目标服务器上执行任意代码。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  CVE-2021-44228

- **漏洞类型**

  代码执行

- **检测规则**

103020429

- **受影响版本**
  - Apache Log4j2 2.x <= 2.14.1
  - Apache Log4j2 2.15.0-rc1
- **修复建议**
  - 目前，Apache 官方已发布新版本完成漏洞修复，建议及时升级至 2.15.0-rc2 以上版本：https://github.com/apache/logging-log4j2/tags
  - 建议同时采用如下临时措施进行漏洞防范：

    添加 jvm 启动参数-Dlog4j2.formatMsgNoLookups=true；

    在应用 classpath 下添加 log4j2.component.properties 配置文件，文件内容为 log4j2.formatMsgNoLookups=true；

    JDK 使用 11.0.1、8u191、7u201、6u211 及以上的高版本；

    部署使用第三方防火墙产品进行安全防护。

2.108 F5 BIG-IP/IQ 远程代码执行漏洞

- **漏洞描述**

  F5 BIG-IP 远程代码执行漏洞(CVE-2023-46747)，未经授权的远程攻击者通过管理端口或自身 IP 地址访问 BIG-IP 系统，利用此漏洞可能绕过身份认证，导致在暴露流量管理用户界面（TMUI）的 F5 BIG-IP 实例上执行任意代码。

- **漏洞标签**

工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  CVE-2021-22986

- **漏洞类型**

  代码执行

- **检测规则**

  106012516

- **受影响版本**
  - BIG-IP 16.x: 16.1.0 - 16.1.2
  - BIG-IP 15.x: 15.1.0 - 15.1.5
  - BIG-IP 14.x: 14.1.0 - 14.1.4
  - BIG-IP 13.x: 13.1.0 - 13.1.4
  - BIG-IP 12.x: 12.1.0 - 12.1.6
  - BIG-IP 11.x: 11.6.1 - 11.6.5
- **修复建议**
  - 建议将 F5 BIG-IP / BIG-IQ 升级至安全版本。下载地址参考：https://support.f5.com/csp/article/K02566623
  - 建议利用阿里云安全组功能为 F5 BIG-IP / BIG-IQ 相关管理界面设置白名单，仅对可信地址开放访问。

2.109 Exchange 服务端请求伪造漏洞

- **漏洞描述**

  Exchange 中身份验证后的任意文件写入漏洞。攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。该漏洞可以配合 CVE-2021-26855 SSRF 漏洞进行组合攻击。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  CVE-2021-26855

- **漏洞类型**

  代码执行

- **检测规则**

  106055950

- **受影响版本**
  - exchange: 2010/2013/2016/2019

- **修复建议**
  - 微软已发布相关安全更新，用户可跟进以下链接进行升级：

    https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

2.110 Exchange 任意文件写入漏洞

- **漏洞描述**

  Exchange 中身份验证后的任意文件写入漏洞。攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。该漏洞可以配合 CVE-2021-26855 SSRF 漏洞进行组合攻击。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备

- **漏洞编号**

  CVE-2021-27065

- **漏洞类型**

  代码执行

- **检测规则**

  106052987

- **受影响版本**
  - exchange: 2010/2013/2016/2019
- **修复建议**
  - 微软已发布相关安全更新，用户可跟进以下链接进行升级：

    https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

2.111 vCenter Server 远程执行代码漏洞

- **漏洞描述**

  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，从而在服务器上写入 webshell，最终造成远程任意代码执行。

- **漏洞标签**

  工具/武器化成熟、漏洞细节公开、漏洞价值大、服务器权限

- **漏洞编号**

  CVE-2021-21972

- **漏洞类型**

  代码执行

- **检测规则**

  106058068

- **受影响版本**

  - VMware vCenter Server 7.0 系列 < 7.0.U1c
  - VMware vCenter Server 6.7 系列 < 6.7.U3l
  - VMware vCenter Server 6.5 系列 < 6.5 U3n
  - VMware ESXi 7.0 系列 < ESXi70U1c-17325551
  - VMware ESXi 6.7 系列 < ESXi670-202102401-SG
  - VMware ESXi 6.5 系列 < ESXi650-202102101-SG

- **修复建议**

  - vCenter Server7.0 版本升级到 7.0.U1c；
  - vCenter Server6.7 版本升级到 6.7.U3l；
  - vCenter Server6.5 版本升级到 6.5 U3n。

2.112 SonicWall SSL-VPN 远程命令执行漏洞

- **漏洞描述**

  SonicWall SSL-VPN 历史版本中存在漏洞，远程攻击者利用 CGI 程序处理逻辑漏洞，构造恶意的 User-Agent，可造成远程任意命令执行，并获得主机控制权限。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  暂无

- **漏洞类型**

  代码执行

- **检测规则**

  106046342

- **受影响版本**

  - SonicWall SSL-VPN< 8.0.0.4

- **修复建议**

  - 升级到 Sonic SMA 8.0.0.4。

2.113 WebLogic 远程代码执行漏洞

- **漏洞描述**

  CVE-2021-2109 中，攻击者可构造恶意请求，造成 JNDI 注入，执行任意代码，从而控制服务器。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  CVE-2021-2109

- **漏洞类型**

  代码执行

- **检测规则**

  103003814

- **受影响版本**
  - WebLogic 10.3.6.0.0
  - WebLogic 12.1.3.0.0
  - WebLogic 12.2.1.3.0
  - WebLogic 12.2.1.4.0
  - WebLogic 14.1.1.0.0
- **修复建议**
  - 升级 Weblogic Server 运行环境的 JDK 版本；
  - 升级官方安全补丁，参考 Oracle 官网发布的补丁：Oracle Critical Patch Update Advisory - January 2021。

2.114 JumpServer 远程命令执行漏洞

- **漏洞描述**

  JumpServer 是一款完全开源的堡垒机，使用 GNU GPL v2.0 开源协议，是符合 4A 的专业运维审计系统。

  该漏洞由于一些接口未做授权限制，攻击者可构造恶意请求获取敏感信息，或者执行任意命令。

- **漏洞标签**

  影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

- **漏洞编号**

  暂无

- **漏洞类型**

  命令执行

- **检测规则**

  106054833

- **受影响版本**
  - JumpServer 堡垒机＜v2.6.2 版本

- JumpServer 堡垒机＜v2.5.4 版本
- JumpServer 堡垒机＜v2.4.5 版本

➢ **修复建议**

- 官方已发布漏洞修复版本，建议 JumpServer 堡垒机（含社区版及企业版）用户升级至安全版本。

2.115 SaltStack 命令执行漏洞

➢ **漏洞描述**

该漏洞由于 SALT-NETAPI 不正确地验证了 EAUTH 凭据和令牌导致，任何“ EAUTH”或“ TOKEN”的值都将允许用户绕过身份验证并调用 SALT SSH。未经身份验证的用户可以访问针对 Salt-SSH 名册中设置的目标运行命令。

➢ **漏洞标签**

影响范围广、工具/武器化成熟、历史重大漏洞、红队打点必备、服务器权限、漏洞价值大、软件供应链风险

➢ **漏洞编号**

CVE-2020-25592

➢ **漏洞类型**

命令执行

➢ **检测规则**

103046105

➢ **受影响版本**

- SaltStack 2015/2016/2017/2018/2019/3000/3001/3002

➢ **修复建议**

- SaltStack 官方已发布安全补丁，腾讯云安全建议您尽快更新安全补丁，避免影响业务。补丁下载链接：https://gitlab.com/saltstack/open/salt-patches
- 从 SaltStack 官方下载安全软件版本，下载地址：https://repo.saltstack.com/

2.116 XXL-JOB 未授权接口反序列化漏洞

➢ 漏洞描述

XXL-JOB 的 Restful API 接口或 RPC 接口没有配置认证措施，未授权的攻击者可构造恶意请求，造成远程执行命令

➢ 漏洞标签

工具/武器化成熟、历史重大漏洞、红队打点必备

➢ 漏洞编号

暂无

➢ 漏洞类型

代码执行

➢ 检测规则

106053257

➢ 受影响版本

- XXL-JOB <= 2.2.0

➢ 修复建议

- 开启 XXL-JOB 自带的鉴权组件：官方文档中搜索“xxl.job.accessToken”，按照文档说明启用即可；
- 端口访问限制：通过配安全组限制只允许指定 IP 才能访问端口。

2.117 Apache Flink 目录遍历漏洞

➢ 漏洞描述

Apache Flink 声明式的数据分析开源系统，结合了分布式 MapReduce 类平台的高效，灵活的编程和扩展性,具有强大的流处理和批处理功能。同时在并行数据库发现查询优化方案。

➢ 漏洞标签

工具/武器化成熟、涉及 HVV 重点系统、漏洞细节公开

➢ 漏洞编号

CVE-2020-17518/17519

- **漏洞类型**

  目录遍历

- **检测规则**

  103022959

- **受影响版本**

  - Apache Flink 1.11.0
  - Apache Flink 1.11.1
  - Apache Flink 1.11.2

- **修复建议**

  - 升级 Flink 版本至 1.11.3 及以上。

2.118 Apache Solr ConfigSet API 文件上传漏洞

- **漏洞描述**

  Solr 是一个独立的企业级搜索应用服务器，它对外提供类似于 Web-service 的 API 接口。用户可以通过 http 请求，向搜索引擎服务器提交一定格式的 XML 文件，生成索引；也可以通过 Http Get 操作提出查找请求，并得到 XML 格式的返回结果。

- **漏洞标签**

  影响范围广、利用条件简单、漏洞价值大

- **漏洞编号**

  CVE-2020-13957

- **漏洞类型**

  文件上传

- **检测规则**

  101003145

- **受影响版本**

  - Apache Solr 6.6.0 -6.6.5
  - Apache Solr 7.0.0 -7.7.3
  - Apache Solr 8.0.0 -8.6.2

- **修复建议**
  - 升级到最新版本：

    http://archive.apache.org/dist/lucene/solr/