攻防演练必修高危漏洞合集

（2023.08）

浙江省大数据发展管理局

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电子政务系统的影子资产增多，高危风险漏洞一直是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，很多单位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。

本期报告整合了近两年在攻防演练被红队利用最频繁且危害较高的漏洞，包含了详细的漏洞基础信息、检测规则和修复方案，各地可根据自身资产情况进行针对性的排查、补丁升级、配置封堵策略和防御策略优化等相关工作。

目　录

1. 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

Apache Log4j2 2.15.0-rc1

4) 检测规则

查看是否存在类似${jndi:相关请求流量。

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-rc2

官方下载链接：

https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2

建议同时采用如下临时措施进行漏洞防范：

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

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

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

4.部署使用第三方防火墙产品进行安全防护。

2. 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。

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

升级到 FastJosn v2：

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

3. 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。

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

同时建议将 NameServer、Broker 等组件部署在内网，并增加权限认证。

4. 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。

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

5. 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/cgi-bin/.%2e/.%2e/.%2e/.%2e 或/icons/.%2e/%2e%2e/%2e%2e/%2e%2e 相关字样。

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

6. 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。

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

7. 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。

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

8. Apache Druid 远程代码执行漏洞 CVE-2023-25194

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。

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

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。ApacheRocketMQ 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。

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/

10. 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。

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

11. 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。

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

12. 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 ;

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。

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

13. 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。

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/download

14. nginxWebUI 远程命令执行漏洞（AVD-2023-1672641）

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=

5) 修复方案

1.通过设置安全组功能，仅对可信地址和内网开放 nginxWebUI 来缓解风险。

2. 官方已发布漏洞补丁及修复版本，但组件修复不完全，防护机制可被绕过， 且其他接口仍存在多个高危漏洞。

因此建议受漏洞影响的用户及时关注厂商公告并及时更新 NginxWebUI：

http://file.nginxwebui.cn/nginxWebUI-3.6.5.jar

15. Swagger-ui 未授权访问漏洞

1) 漏洞描述

Swagger 是一个规范和完整的框架，用于生成、描述、调用和可视化 RESTful 风格的 Web 服务。总体目标是使客户端和文件系统作为服务器以同样的速度来更新。相关的方法，参数和模型紧密集成到服务器端的代码，允许 API 来始终保持同步。Swagger-UI 会根据开发人员在代码中的设置来自动生成 API 说明文档，若存在相关的配置缺陷，攻击者可以未授权翻查 Swagger 接口文档，得到系统功能 API 接口的详细参数，再构造参数发包，通过回显获取系统大量的敏感信息。

2) 披露时间

未知

3) 影响版本

v1、V2、v3 所有版本

4) 检测规则

可利用未授权访问漏洞，直接访问以下链接：

/api

/api-docs

/api-docs/swagger.json

/api.html

/api/api-docs

/api/apidocs

/api/doc

/api/swagger

/api/swagger-ui

/api/swagger-ui.html

/api/swagger-ui.html/

/api/swagger-ui.json

/api/swagger.json

/api/swagger/

/api/swagger/ui

/api/swagger/ui/

/api/swaggerui

/api/swaggerui/

/api/v1/

/api/v1/api-docs

/api/v1/apidocs

/api/v1/swagger

/api/v1/swagger-ui

/api/v1/swagger-ui.html

/api/v1/swagger-ui.json

/api/v1/swagger.json

/api/v1/swagger/

/api/v2

/api/v2/api-docs

/api/v2/apidocs

/api/v2/swagger

/api/v2/swagger-ui

/api/v2/swagger-ui.html

/api/v2/swagger-ui.json

/api/v2/swagger.json

/api/v2/swagger/

/api/v3

/apidocs

/apidocs/swagger.json

/doc.html

/docs/

/druid/index.html

/graphql

/libs/swaggerui

/libs/swaggerui/

/spring-security-oauth-resource/swagger-ui.html

/spring-security-rest/api/swagger-ui.html

/sw/swagger-ui.html

/swagger

/swagger-resources

/swagger-resources/configuration/security

/swagger-resources/configuration/security/

/swagger-resources/configuration/ui

/swagger-resources/configuration/ui/

/swagger-ui

/swagger-ui.html

/swagger-ui.html#/api-memory-controller

/swagger-ui.html/

/swagger-ui.json

/swagger-ui/swagger.json

/swagger.json

/swagger.yml

/swagger/

/swagger/index.html

/swagger/static/index.html

/swagger/swagger-ui.html

/swagger/ui/

/Swagger/ui/index

/swagger/ui/index

/swagger/v1/swagger.json

/swagger/v2/swagger.json

/template/swagger-ui.html

/user/swagger-ui.html

/user/swagger-ui.html/

/v1.x/swagger-ui.html

/v1/api-docs

/v1/swagger.json

/v2/api-docs

/v3/api-docs

5) 修复方案

1.配置 Swagger 开启页面访问限制。

2.排查接口是否存在敏感信息泄露（例如：账号密码、SecretKey、OSS 配置等），若有则进行相应整改。

16. 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。

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/

17. 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。

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

18. 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

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

19. 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

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		点击下载

	iDS-2SK8xxxx		
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 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		点击下载
41	DS-76xxN-Exx DS-78xxN-Kxx DS-NVR-K1xx DS-NVR-K2xx	V4.30.210 Build201224- 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。

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/

20. 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。

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

21. 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。

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。

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

22. 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。

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

23. 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。

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

24. 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

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

25. 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。

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

26. 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。

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

27. 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。

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/

28. 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。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。

5) 修复方案

联系官方尽早升级到最新版本：https://www.h3c.com/cn/

29. 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。

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/

30. Nacos 反序列化漏洞 CNVD-2023-45001

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。

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

建议同时采用如下临时措施进行漏洞防范：

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。

31. 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。

建议同时采用如下临时措施进行漏洞防范：

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：

1. 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。

2. 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。

32. Vmware vcenter 远程代码执行漏洞 CVE-2021-21972

1) 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。

2) 披露时间

2021 年 2 月 24 日

3）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

4) 检测规则

检查流量中是否有对/ui/vropspluginui/rest/services/updateova 的请求，如果 404，则代表不存在漏洞，如果 200，则代表存在漏洞。

5) 修复方案

1.升级 VMware vCenter Server 与 VMware ESXi 至最新版本。

2.针对 CVE-2021-21972 VMware vCenter Server 远程代码漏洞与 CVE-2021-21973 VMware vCenter Server SSRF 漏洞，可按照 https://kb.vmware.com/s/article/82374 相关措施进行缓解。

3.针对 CVE-2021-21974 VMware ESXI 堆溢出漏洞，可按照 https://kb.vmware.com/s/article/76372 相关措施进行缓解。

33. 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。

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/

建议同时采用如下临时措施进行漏洞防范：

可在 module/common/model.php 文件中 echo $endResponseException->getContent();后面加上 exit(); 来修复权限绕过漏洞。