亚信安全

# 2023
# 攻防演练利器之必修高危漏洞合集

红队视角，牢筑防线



亚信安全科技股份有限公司 - 应急响应中心

2023年7月

www.asiainfo-sec.com

护航产业互联 安全数字世界

# 目 录

# 一、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 40 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。

# 二、漏洞详情

## 2.1 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

### ➢ 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：

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。

## 2.2 Fastjson 远程代码执行漏洞

### ➢ 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

### ➢ 受影响版本

- Fastjson ≤ 1.2.80

### ➢ 修复建议

1、升级至版本 FastJson 1.2.83：

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

2、升级到 FastJosn v2：

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

## 2.3 Atlassian Confluence 远程代码执行漏洞

### ➢ 漏洞描述

远程攻击者在未经身份验证的情况下，可构造 OGNL 表达式进行注入，实现在 Confluence Server 或 Data Center 上执行任意代码。

### ➢ 漏洞标签

工具/武器化成熟、历史重大漏洞、服务器权限

### ➢ 漏洞编号

CVE-2022-26134

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- Confluence Server / Data Center 1.3.0 < 7.4.17
- Confluence Server / Data Center 7.13.0 < 7.13.7
- Confluence Server / Data Center 7.14.0 < 7.14.3
- Confluence Server / Data Center 7.15.0 < 7.15.2
- Confluence Server / Data Center 7.16.0 < 7.16.4
- Confluence Server / Data Center 7.17.0 < 7.17.4
- Confluence Server / Data Center 7.18.0 < 7.18.1

### ➢ 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，参考官方升级说明，酌情升级至安全版本：

- Confluence Server / Data Center >= 7.4.17
- Confluence Server / Data Center >= 7.13.7
- Confluence Server / Data Center >= 7.14.3
- Confluence Server / Data Center >= 7.15.2
- Confluence Server / Data Center >= 7.16.4
- Confluence Server / Data Center >= 7.17.4
- Confluence Server / Data Center >= 7.18.1

## 2.4 Apache Commons Text 远程代码执行漏洞

### ➢ 漏洞描述

当使用 Apache Commons Text 中的字符串替换功能时，一些可用的插值器可以触发网络访问或代码执行。如果应用程序在传递给替换的字符串中包含用户输入而未对其进行适当清理，则攻击者将允许攻击者触发这些插值器。

### ➢ 漏洞标签

软件供应链风险、历史重大漏洞、工具/武器化成熟、服务器权限

### ➢ 漏洞编号

CVE-2022-42889

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 1.5.0 ≤ Apache Commons Text ＜ 1.10.0

### ➢ 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。

## 2.5 Apache Airflow 远程代码执行漏洞

### ➢ 漏洞描述

Apache Airflow 是一个可编程，调度和监控的工作流平台，基于有向无环图(DAG)，Airflow 可以定义一组有依赖的任务，按照依赖依次执行。当攻击者可访问到 Apache Airflow 的后台 UI，且环境中存在默认 dag 时，可构造恶意请求借助 run_id 执行任意命令。

### ➢ 漏洞标签

服务器权限、漏洞价值大、影响范围广、软件供应链风险、工具/武器化成熟

### ➢ 漏洞编号

CVE-2022-40127

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- Airflow < 2.4.0

### ➢ 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。

## 2.6 ThinkPHP 命令执行漏洞

### ➢ 漏洞描述

该漏洞是由于 Thinkphp 开启了多语言功能，并且对参数 lang 传参过滤不严谨，导致攻击者可利用该漏洞执行命令。

### ➢ 漏洞标签

国产开源框架、服务器权限、漏洞价值大、影响范围广、红队打点必备

### ➢ 漏洞编号

CNVD-2022-86535

### ➢ 漏洞类型

命令执行

### ➢ 受影响版本

- ThinkPHP ThinkPHP >=V6.0.1，<=V6.0.13
- ThinkPHP ThinkPHP >=V5.0.X，<=V5.1.X

### ➢ 修复建议

如不需要多语言功能，请及时关闭此功能，可参考官方文档：

https://www.kancloud.cn/manual/thinkphp6_0/1037637

https://static.kancloud.cn/manual/thinkphp5/118132

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。

## 2.7 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

### ➢ 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：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。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。

## 2.8 禅道项目管理系统远程命令执行漏洞

### ➢ 漏洞描述

禅道项目管理系统存在远程命令执行漏洞，该漏洞源于在认证过程中未正确退出程序，导致了认证绕过，并且后台中有多种执行命令的方式，攻击者可利用该漏洞在目标服务器上注入任意命令，实现未授权接管服务器。

### ➢ 漏洞标签

服务器权限、国产办公系统、国产开源框架、红队打点必备、工具/武器化成熟

### ➢ 漏洞编号

CNVD-2023-02709

### ➢ 漏洞类型

命令执行

### ➢ 受影响版本

- 杭州易软共创网络科技有限公司 禅道项目管理系统 >=17.4，<=18.0.beta1（开源版）
- 杭州易软共创网络科技有限公司 禅道项目管理系统 >=7.4，<=8.0.beta1（企业版）

- 杭州易软共创网络科技有限公司 禅道项目管理系统 >=3.4，<=4.0.beta1（旗舰版）

### ➢ 修复建议

1、进行官方升级:

具体升级方法:https://www.zentao.net/book/zentaoprohelp/41.html

2、安全产品升级:

部分厂商安全产品具备识别该漏洞功能，进行版本升级至最新版。

3、临时防护措施：

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。

## 2.9 Smartbi 远程命令执行漏洞

### ➢ 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、服务器权限、红队打点必备、国产办公系统

### ➢ 漏洞编号

无

### ➢ 漏洞类型

命令执行

### ➢ 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

## 2.10 Apache Dubbo 反序列化远程代码执行漏洞

### ➢ 漏洞描述

由于 Dubbo 泛型调用中存在反序列化漏洞，未经身份验证的攻击者可以通过构造特殊的请求利用此漏洞，造成远程代码执行，从而获取远程服务器的权限。

### ➢ 漏洞标签

工具/武器化成熟、服务器权限

### ➢ 漏洞编号

CVE-2023-23638

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 2.7.0 <= Apache Dubbo <= 2.7.21
- 3.0.0 <= Apache Dubbo <= 3.0.13
- 3.1.0 <= Apache Dubbo <= 3.1.5

### ➢ 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，建议您在升级前做好数据备份工作，避免出现意外。

https://github.com/apache/dubbo/releases

1.限制用户输入，过滤恶意数据，可以减少攻击者利用反序列化漏洞的可能性。

2.配置黑白名单，限制可序列化的类集合。

3.使用 Java 的安全管理器（SecurityManager）来限制反序列化操作的权限，例如限制访问文件系统、网络等操作。

## 2.11 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

无

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- Apache Druid <= 25.0.0

### ➢ 修复建议

1. 避免 Apache Druid 开放至公网。
2. 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

## 2.12 瑞友天翼应用虚拟化系统远程代码执行漏洞

### ➢ 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

无

### ➢ 漏洞类型

代码执行

### ➢ 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

1.避免将该系统开放至公网。

2.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

## 2.13 Apache Superset 身份认证绕过漏洞

### ➢ 漏洞描述

这个漏洞是由于默认配置的 SECRET_KEY 不安全所导致的。如果管理员没有根据安装说明更改默认配置的 SECRET_KEY，则攻击者可以通过身份验证并访问未经授权的资源或执行恶意代码

### ➢ 漏洞标签

工具/武器化成熟、利用条件简单

### ➢ 漏洞编号

CVE-2023-27524

### ➢ 漏洞类型

认证绕过

### ➢ 受影响版本

- Apache Superset <= 2.0.1

### ➢ 修复建议

1. 修改默认的 SECRET_KEY,参考官方文档:
https://superset.apache.org/docs/installation/configuring-superset/#secret_key-rotation
2. 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://downloads.apache.org/superset/

## 2.14 Apache Solr 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

### ➢ 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

## 2.15 Apache RocketMQ 远程代码执行漏洞

### ➢ 漏洞描述

RocketMQ 5.1.0 及以下版本在一定条件下存在远程命令执行风险。RocketMQ 的 NameServer、Broker、Controller 等多个组件暴露在外网且缺乏权限验证，攻击者可以利用此缺陷通过「更新配置」功能修改配置路径，进而以系统用户身份执行任意命令（伪造 RocketMQ 协议也可执行任意命令）。

### ➢ 漏洞标签

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

### ➢ 漏洞编号

CVE-2023-33246

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 5.0.0 <= Apache RocketMQ <= 5.1.0
- 4.0.0 <= Apache RocketMQ <= 4.9.5

### ➢ 修复建议

1.RocketMQ 的 NameServer、Broker、Controller 组件非必要不暴露在公网。同时，建议增加访问权限认证。

2.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://rocketmq.apache.org/download。

## 2.16 NginxWebUI runCmd 远程代码执行漏洞

### ➢ 漏洞描述

该漏洞源于开发人员没有对 runCmd 接口处传入的参数进行有效过滤，攻击者可在无需登录的情况下绕过路由权限校验，通过拼接语句的方式执行任意命令，最终控制服务器。

### ➢ 漏洞标签

工具/武器化成熟、服务器权限、历史重大漏洞、影响范围广

### ➢ 漏洞编号

无

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- nginxWebUI < 3.5.1

P.S. v3.5.1 版本修复了登陆绕过漏洞，但是 RCE 漏洞在最新版本（v3.6.5）中仍可绕过防护进行利用

### ➢ 修复建议

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

## 2.17 Smartbi 商业智能软件绕过登录漏洞

### ➢ 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

无

### ➢ 漏洞类型

认证绕过

### ➢ 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

## 2.18 Nacos 集群 Raft 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

### ➢ 受影响版本

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

### ➢ 修复建议

1.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。

2.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

## 2.19 Atlassian Confluence OGNL 表达式注入漏洞

### ➢ 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

命令执行

### ➢ 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

1. 升级 Atlassian Confluence Server and Data Center 至安全版本。

2. 临时缓解方案：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。

https://packages.atlassian.com/maven-internal/opensymphony/xwork/1.0.3-atlassian-10/xwork-1.0.3-atlassian-10.jar

## 2.20 F5 BIG-IP iControl REST 身份验证绕过漏洞

### ➢ 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

认证绕过

### ➢ 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：

1. 通过自身 IP 地址阻止 iControl REST 访问。
2. 通过管理界面阻止 iControl REST 访问。
3. 修改 BIG-IP httpd 配置。

## 2.21 Apache CouchDB 权限提升漏洞

### ➢ 漏洞描述

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：

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。

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。

### ➢ 漏洞标签

影响范围广、漏洞细节公开、服务器权限、红队打点必备

### ➢ 漏洞编号

CVE-2022-24706

### ➢ 漏洞类型

权限提升

### ➢ 受影响版本

- Apache CouchDB <3.2.2

### ➢ 修复建议

厂商已发布补丁修复漏洞，用户请尽快更新至安全版本：Apache CouchDB 3.2.2 及更高版本。

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。

与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

## 2.22 Atlassian Bitbucket Data Center 远程代码执行漏洞

### ➢ 漏洞描述

Atlassian Bitbucket Data Center 存在远程代码执行漏洞。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。

### ➢ 漏洞标签

漏洞细节公开、利用条件简单、漏洞价值大、数据库权限

### ➢ 漏洞编号

CVE-2022-26133

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 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

### ➢ 修复建议

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

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

## 2.23 Linux Kernel 本地权限提升漏洞

### ➢ 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

权限提升

### ➢ 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

## 2.24 Sapido 多款路由器命令执行漏洞

### ➢ 漏洞描述

Sapido 路由器存在命令执行漏洞，攻击者可通过未授权进入命令执行页面，进而可以 root 权限执行任意命令。

### ➢ 漏洞标签

漏洞细节公开、利用条件简单、服务器权限

### ➢ 漏洞编号

无

### ➢ 漏洞类型

命令执行

### ➢ 受影响版本

- BR270n-v2.1.03
- BRC76n-v2.1.03
- GR297-v2.1.3
- RB1732-v2.0.43

### ➢ 修复建议

1. 尽量不要使用命令执行函数。
2. 客户端提交的变量在进入执行命令函数前要做好过滤和检测。
3. 在使用动态函数之前，确保使用的函数是指定的函数之一。
4. 对 PHP 语言来说，不能完全控制的危险函数最好不要使用。

## 2.25 向日葵远程代码执行漏洞

### ➢ 漏洞描述

上海贝锐信息科技股份有限公司的向日葵远控软件存在远程代码执行漏洞（CNVD-2022-10270/CNVD-2022-03672），安装以下存在 windwos 问题版本的个人版和简约版，攻击者可利用该漏洞获取服务器控制权。

### ➢ 漏洞标签

社会工程学攻击、工具/武器化成熟

### ➢ 漏洞编号

CNVD-2022-10270

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 向日葵个人版　for Windows <= 11.0.0.33

- 向日葵简约版　<= V1.0.1.43315（2021.12）

### ➢ 修复建议

向日葵漏洞防护为大家找到的解决远程代码执行漏洞的方法有:

1. 输入检查:应用程序必须实现输入检查机制，将所有从外部接收的数据都进行严格的检查和过滤，防止恶意代码被注入。

2. 参数化查询:采用参数化查询可以防止攻击者通过利用应用程序的注入漏洞来修改查询语句，实现任意代码执行的攻击。

3. 输出编码:在输出时对敏感字符进行编码保护，比如 HTML 编码，防止恶意代码直接输出执行。

4. 使用最新的安全防护措施:保证服务器系统和应用程序的所有组件、库和插件都是最 新的，确保已知的漏洞都得到修复。

5. 强制访问控制:应该设置访问控制机制，确保恶意用户无法访问敏感数据和代码。

## 2.26 Apache Kafka Connect JNDI 注入漏洞

### ➢ 漏洞描述

由于 Apache Kafka Connect 中存在 JNDI 注入漏洞，当 Kafka Connect Worker 允许远程访问且可以创建或修改连接器时，恶意攻击者可通过修改连接器的 Kafka 客户端属性配置，从而进行 JNDI 注入攻击或反序列化利用，成功利用此漏洞可在目标服务器上执行任意代码，获取目标服务器的控制权限。

### ➢ 漏洞标签

影响范围广、服务器权限、红队打点必备、利用条件简单

### ➢ 漏洞编号

CVE-2023-25194

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 2.3.0 <= Apache Kafka <= 3.3.2

### ➢ 修复建议

目前官方已修复该漏洞，受影响用户可以升级更新到安全版本。官方下载链接：

https://kafka.apache.org/downloads

## 2.27 Apache HTTP Server 请求走私漏洞

### ➢ 漏洞描述

Apache HTTP Server 版本 2.4.0 - 2.4.55 的某些 mod_proxy 配置可能导致 HTTP 请求走私攻击，这种攻击可能会导致绕过代理服务器中的访问控制，将非预期的 URL 代理到现有源服务器，以及缓存中毒等。

### ➢ 漏洞标签

影响范围广、利用条件简单、服务器权限、红队打点必备

### ➢ 漏洞编号

CVE-2023-25690

### ➢ 漏洞类型

HTTP 请求走私

### ➢ 受影响版本

- 2.4.0<= Apache HTTP Server 版本<= 2.4.55

### ➢ 修复建议

目前该漏洞已经修复，受影响用户可升级到以下版本：

Apache HTTP Server 版本 >= 2.4.56

下载链接：

https://httpd.apache.org/download.cgi

注：Apache HTTP Server 版本 2.4.56 中还修复了通过 mod_proxy_uwsgi 的 HTTP 响应走私漏洞（CVE-2023-27522，中危），该漏洞影响了 Apache HTTP Server 版本 2.4.30 - 2.4.55。

## 2.28 Spring Framework 安全绕过漏洞

### ➢ 漏洞描述

在带有 mvcRequestMatcher 的 Spring Security 配置中使用无前缀双通配符模式会导致 Spring Security 和 Spring MVC 之间的模式匹配不匹配，并可能导致安全绕过。

### ➢ 漏洞标签

影响范围广、涉及 HVV 重点系统、利用条件简单、服务器权限、红队打点必备

### ➢ 漏洞编号

CVE-2023-20860

### ➢ 漏洞类型

认证绕过

### ➢ 受影响版本

- 6.0.0 - 6.0.6、5.3.0 - 5.3.25（注：5.3 之前的版本不受影响）

### ➢ 修复建议

受影响用户及时更新升级到以下修复版本：

- Spring Framework >= 6.0.7
- Spring Framework >= 5.3.26

下载链接：

https://spring.io/projects/spring-framework

## 2.29 Microsoft Outlook 权限提升漏洞

### ➢ 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

认证绕过

### ➢ 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：

1、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

2、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。

## 2.30 MinIO 信息泄露漏洞

### ➢ 漏洞描述

在集群部署的 MinIO 中，未经身份认证的远程攻击者通过发送特殊 HTTP 请求即可获取所有环境变量，其中包括 MINIO_SECRET_KEY 和 MINIO_ROOT_PASSWORD，造成敏感信息泄露，最终可能导致攻击者以管理员身份登录 MinIO。

### ➢ 漏洞标签

涉及 HVV 重点系统、红队打点必备

### ➢ 漏洞编号

CVE-2023-28432

### ➢ 漏洞类型

信息泄露

### ➢ 受影响版本

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

### ➢ 修复建议

目前官方已发布安全修复版本，受影响用户可以升级到 RELEASE.2023-03-20T20-16-18Z 及以上版本。

https://github.com/minio/minio/releases/tag/RELEASE.2023-03-20T20-16-18Z

临时修复方案，在 waf/ips 等安全产品上配置策略，拒绝所有 post 到 /minio/bootstrap/v1/verify 流量。

## 2.31 畅捷通 T+ 前台远程命令执行漏洞

### ➢ 漏洞描述

由于畅捷通 T+前台存在反序列化漏洞，恶意攻击者成功利用此漏洞可在目标服务器上执行任意命令。

### ➢ 漏洞标签

漏洞细节公开、利用条件简单、服务器权限、国产办公系统、红队打点必备

### ➢ 漏洞编号

无

### ➢ 漏洞类型

命令执行

### ➢ 受影响版本

- T+13.0、T+16.0

### ➢ 修复建议

目前官方已修复该漏洞，受影响用户可以升级更新到安全版本。官方下载链接：

https://www.chanjetvip.com/product/goods/

## 2.32 泛微 e-cology 前台任意用户登录漏洞

### ➢ 漏洞描述

泛微 e-cology 前台任意用户登录漏洞：泛微 e-cology9 部分版本中存在前台任意用户登录漏洞。该漏洞允许未经身份验证的攻击者通过发送构造的请求触发漏洞，成功利用此漏洞的攻击者可登录任意用户。

### ➢ 漏洞标签

漏洞细节公开、利用条件简单、国产办公系统、红队打点必备

### ➢ 漏洞编号

无

### ➢ 漏洞类型

认证绕过

### ➢ 受影响版本

- 部分 e-cology9 并且补丁版本 ＜10.57

### ➢ 修复建议

目前，官方已发布修复建议，建议受影响的用户尽快升级至最新版本的补丁。下载地址：

https://www.weaver.com.cn/cs/securityDownload.asp#

## 2.33 Openfire 控制台权限绕过漏洞

### ➢ 漏洞描述

Openfire 的管理控制台是一个基于 Web 的应用程序，被发现可以使用路径遍历的方式绕过权限校验。成功利用后，未经身份验证的用户可以访问 Openfire 管理控制台中的后台页面。同时由于 Openfire 管理控制台的后台提供了安装插件的功能，所以攻击者可以通过安装恶意插件达成远程代码执行的效果。

### ➢ 漏洞标签

漏洞细节公开、利用条件简单、服务器权限、红队打点必备

### ➢ 漏洞编号

CVE-2023-32315

### ➢ 漏洞类型

认证绕过

### ➢ 受影响版本

- 3.10.0 <= Openfire < 4.6.8、4.7.5

### ➢ 修复建议

临时缓解方案：

使用网络 ACL 限制访问控制台的来源，而且建议如非必要，不要将 Openfire 管理控制台暴露在互联网上。

升级修复方案：

该问题已在 Openfire 的 4.7.4 和 4.6.8 版本中得到修补，建议升级到不受漏洞影响的版本。

## 2.34 Apache RocketMQ 远程代码执行漏洞

### ➢ 漏洞描述

此漏洞是由于 CVE-2023-33246 补丁未修复完全，当 RocketMQ 的 NameServer 组件暴露在外网，且缺乏有效的身份认证时，攻击者可以利用更新配置功能，以 RocketMQ 运行的系统用户身份执行任意命令。

### ➢ 漏洞标签

影响范围广、漏洞细节公开、漏洞价值大、红队打点必备、近期爆发漏洞

### ➢ 漏洞编号

CVE-2023-37582

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- RocketMQ < 4.9.7
- RocketMQ < 5.1.2

### ➢ 修复建议

目前官方已发布安全版本，建议受影响用户升级至：

- RocketMQ 5.x >= 5.1.2
- RocketMQ 4.x >= 4.9.7

官方补丁下载地址：

https://rocketmq.apache.org/download/

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

## 2.35 用友 NC Cloud 远程代码执行漏洞

### ➢ 漏洞描述

用友 NC 及 NC Cloud 系统存在任意文件上传漏洞，攻击者可通过 uapjs（jsinvoke）应用构造恶意请求非法上传后门程序，此漏洞可以给 NC 服务器预埋后门，从而可以随意操作服务器。

### ➢ 漏洞标签

漏洞细节公开、涉及 HVV 重点系统、服务器权限、国产办公系统、近期爆发漏洞

### ➢ 漏洞编号

无

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- NC63、NC633、NC65
- NC Cloud1903、NC Cloud1909
- NC Cloud2005、NC Cloud2105、NC Cloud2111
- YonBIP 高级版 2207

### ➢ 修复建议

1.官方已经发布修复补丁，请进行升级。
2.或者进行 waf 等安全部署拦截恶意字符

## 2.36 Gitlab 远程代码执行漏洞

### ➢ 漏洞描述

GitLab 某些端点的路径存在无需授权风险，攻击者可在无需认证的情况下完成图片上传，并利用该漏洞构造恶意数据执行远程命令，最终造成服务器敏感信息泄露或执行任意命令。

### ➢ 漏洞标签

影响范围广、工具/武器化成熟、漏洞价值大、软件供应链风险

### ➢ 漏洞编号

CVE-2021-22205

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 11.9 <= GitLab（CE/EE）< 13.8.8
- 13.9 <= GitLab（CE/EE）< 13.9.6
- 13.10 <= GitLab（CE/EE）< 13.10.3

### ➢ 修复建议

1、设置 Gitlab 仅对可信地址开放；

2、升级至安全版本：

GitLab（CE/EE） >= 13.8.8

GitLab（CE/EE） >= 13.9.6

GitLab（CE/EE） >= 13.10.3

## 2.37 Vmware vcenter 远程代码执行漏洞

### ➢ 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、涉及 HVV 重点系统、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

### ➢ 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

## 2.38 金蝶 K3Cloud 反序列化漏洞

### ➢ 漏洞描述

由于金蝶云星空能够使用 format 参数指定数据格式为二进制，攻击者可以通过发送由 BinaryFormatter 恶意序列化后的数据让服务端进行危险的 BinaryFormatter 反序列化操作。反序列化过程中没有对数据进行签名或校验，导致攻击者可以在未授权状态下进行服务器远程代码执行。

### ➢ 漏洞标签

涉及 HVV 重点系统、漏洞价值大、服务器权限、国产办公系统

### ➢ 漏洞编号

无

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 金蝶云星空 ＜6.2.1012.4
- 7.0.352.16＜ 金蝶云星空 ＜7.7.0.202111
- 8.0.0.202205＜ 金蝶云星空 ＜8.1.0.20221110

### ➢ 修复建议

目前官方已发布安全补丁，受影响用户可以联系官方获取补丁。

https://vip.kingdee.com/knowledge/specialDetail/352491453127123200?category=352491970117034240&id=388994085535220992&productLineId=1

缓解方案:

对于低于 PT123230 [6.2.1012.4]版本的金蝶云星空：

请禁止把金蝶云星空管理中心发布到公网访问，并使用防火墙设置能访问管理中心的 IP 白名单。如有需要发布到外网，或内网需要访问管理中心，可设置白名单进行控制，详情可参考：

https://vip.kingdee.com/article/248777993676668672?productLineId=1&isKnowledge=2

## 2.39 蓝凌 oa 远程代码执行漏洞

### ➢ 漏洞描述

蓝凌 OA sysSearchMain.do 文件 存在任意文件写入漏洞，攻击者获取后台权限后可通过漏洞写入任意文件，也可以通过 custom.jsp 文件未授权写入恶意文件。

### ➢ 漏洞标签

涉及 HVV 重点系统、漏洞细节公开、服务器权限、国产办公系统

### ➢ 漏洞编号

无

### ➢ 漏洞类型

代码执行

### ➢ 受影响版本

- 未知

### ➢ 修复建议

及时更新到最新版本。

## 2.40 Foxit PDF Reader 及 Editor 任意代码执行漏洞

### ➢ 漏洞描述

Foxit PDF Reader 及 Editor 中存在任意代码执行漏洞，由于 Foxit PDF Reader/Editor 未验证 exportXFAData 方法中的 cPath 参数，使得恶意的.hta 文件写入 Startup 目录中，攻击者可通过诱导受害者打开特制的 PDF 文档触发此漏洞，系统重启后将执行攻击者的恶意代码。

### ➢ 漏洞标签

影响范围广、涉及 HVV 重点系统、漏洞细节公开、利用条件简单、社会工程学攻击

## ➢ 漏洞编号

CVE-2023-27363

## ➢ 漏洞类型

代码执行

## ➢ 受影响版本

- 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

## ➢ 修复建议

目前官方已发布可更新版本，受影响用户可通过以下任一步骤进行更新：

1、在 Foxit PDF 阅读器或 Foxit PDF 编辑器中，点击“帮助”>“关于 Foxit PDF 阅读器”或“关于 Foxit PDF 编辑器”>“检查更新”(对于 10 版本或更早的版本，点击“帮助”>“检查更新”)以更新到最新版本。

2、手动下载更新：

https://www.foxit.com/downloads/