斗象科技
TOPHANT

2024

HW 必修高危漏洞集合

版本：v3.0 | 2024.06

斗象科技 - 漏洞情报中心
Email: service@tophant.com
Tel: 400-156-9866

Make Security Entrenched Still

让安全无法撼动

目录 CONTENTS

一、 前言

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

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

本次报告整合了自 2023 年 8 月份至 2023 年 11 月份在攻防演练被红队利用最频繁且对企业危害较高的漏洞，包含了详细的漏洞基础信息、检测规则和修复方案，企业可根据自身资产信息进行针对性的排查、配置封堵策略和漏洞修复相关工作。

《2024HW 必修高危漏洞集合》预计将发布三期

第一期《2024HW 必修高危漏洞集合_1.0》收录 2024 年 3 月-2024 年 5 月

第二期《2024HW 必修高危漏洞集合_2.0》收录 2023 年 12 月-2024 年 2 月

第三期《2024HW 必修高危漏洞集合_3.0》收录 2023 年 8 月-2023 年 11 月

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

二、 漏洞汇总数据

本文档为斗象发布的《2024HW 必修高危漏洞集合_3.0》对自 2023 年 8 月至 2023 年 11 月份在攻防演练过程红队利用率比较高的漏洞进行总结汇总，具体的数据如下所示：

- 远程代码执行漏洞

  漏洞数量：8 个

  涉及厂商：深信服、海康威视、安恒、绿盟、深信服、weaver、深圳市蓝凌软件股份有限公司、北京通达信科科技有限公司

- 文件上传

  漏洞数量：6 个

  涉及厂商：DedeCMS、weaver、金蝶软件（中国）有限公司、用友网络科技股份有限公司、泛微、金蝶、

- 不安全的反序列化

  漏洞数量：2 个

  涉及厂商：金蝶、北京畅捷通信息技术有限公司

以下为本次高危漏洞自查列表：

漏洞名称	漏洞类型	所属厂商	影响版本
深信服 应用交付管理系统 login 远程命令执行漏洞	远程代码执行漏洞	深信服	应用交付管理系统
海康威视综合安防管理平台存在 Fastjson 远程命令执行漏洞	远程代码执行漏洞	海康威视	iSecure-Center
安恒明御安全网关 远程代码执行漏洞	远程代码执行漏洞	安恒	明御安全网关
绿盟 SAS 堡垒机 Exec 远程命令执行漏洞	远程代码执行漏洞	绿盟	SAS 堡垒机

深信服下一代防火墙 NGAF login.cgi 文件远程命令执行漏洞	远程代码执行漏洞	深信服	下一代防火墙 NGAF
泛微 e-office welink 远程代码执行漏洞	远程代码执行漏洞	weaver	e-office < 10.0_20230821
蓝凌 OA datajson 命令执行	远程代码执行漏洞	深圳市蓝凌软件股份有限公司	蓝凌 OA
通达 OA getdata 远程命令执行漏洞	远程代码执行漏洞	北京通达信科科技有限公司	通达 OA v11.9 通达 OA v11.10
DedeCMS 文件上传漏洞	任意文件上传	DedeCMS	DedeCMS <= 5.7.109
泛微 OA E-Office uploadify 任意文件上传漏洞	任意文件上传	weaver	Wevar E-Office 10
泛微 OA Ecology upload_file.php 文件上传漏洞	任意文件上传	weaver	e-office
金蝶 EAS uploadLogo.action 接口文件上传漏洞	任意文件上传	金蝶软件（中国）有限公司	金蝶 EAS
用友 U8 Cloud upload.jsp 文件上传漏洞	任意文件上传	用友网络科技股份有限公司	用友 U8 Cloud
用友 NC Cloud uploadChunk 任意文件上传漏洞	任意文件上传	用友网络科技股份有限公司	用友-NC-Cloud
金蝶云星空反序列化	不安全的反	金蝶	金蝶云星空<6.2.1012.4

远程代码执行漏洞	序列化		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
畅捷通 T+ 反序列化漏洞	不安全的反序列化	北京畅捷通信息技术有限公司	畅捷通 T+ 13.0 畅捷通 T+ 16.0

三、 自查高危详情

3.1 深信服 应用交付管理系统 login 远程命令执行漏洞

1) 漏洞描述

深信服应用交付管理系统是由深信服科技股份有限公司开发的一种网络应用交付和流量管理解决方案。

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。

攻击者可以通过利用远程命令执行漏洞，在受影响的系统上执行任意命令，包括系统级别的命令。这使得攻击者可以控制和操作目标系统，获取敏感信息、操纵数据或危害系统的完整性和可用性。

2) 披露时间

2023 年 8 月 29 日

3) 影响版本

深信服 应用交付管理系统

4) 检测规则

检测流量中是否存在以下路径：/rep/login

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.sangfor.com.cn/sec_center/details/70df3b537b2549db86f3f31bda4ec850

若无法进行升级的情况下，请使用该产品的用户进行如下操作：

1.配置防护设备以限制不可信 IP 对/rep/login 的请求：强烈建议在网络架构

中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.tophant.com/detail/1696435834779209728?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCNyVCMSVFNCVCRiVBMSVFNiU5QyU4RCUyMCVFNSVCQSU5NCVFNyU5NCVBOCVFNCVCQSVBNCVFNCVCQiU5OCVFNyVBRSVBMSVFNyU5MCU4NiVFNyVCMyVCQiVFNyVCQiU5RiUyMGxvZ2luJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU1JTkxJUJEJUU0JUJCJUE0JUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.2 海康威视综合安防管理平台存在 Fastjson 远程命令执行漏洞

1) 漏洞描述

综合安防管理平台基于“统一软件技术架构”理念设计，采用业务组件化技术，满足平台在业务上的弹性扩展。该平台适用于全行业通用综合安防业务，对各系统资源进行了整合和集中管理，实现统一部署、配置、管理和调度

海康威视综合安防管理平台存在 Fastjson 远程命令执行漏洞，该漏洞可执行系统命令，直接获取服务器权限。

2) 爆发时间

2023 年 9 月 1 日

3) 影响版本

iSecure-Center

4) 检测规则

检测流量中是否存在以下路径：/bic/ssoService/v1/applyCT

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/

若无法进行升级的情况下，请使用该产品的用户进行如下操作：

1.配置防护设备以限制不可信 IP 对该/bic/ssoService/v1/applyCT 的请求：强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.tophant.com/detail/1697503872739840000?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCNSVCNyVFNSVCQSVCNyVFNSVBOCU4MSVFOCVBNyU4NiVFNyVCQiVCQyVFNSU5MCU4OCVFNSVBRSU4OSVFOSU5OCVCMiVFNyVBRSVBMSVFNyU5MCU4NiVFNSVCOSVCMyVFNSU4RiVCMCVFNSVBRCU5OCVFNSU5QyVBOEZhc3Rqc29uJUU4JUJGJTlDJUU3JUE4JThCJUU1JTkxJUJEJUU0JUJCJTg5JUE3JUU4JUFFJUExJThDJUU2JUI0JUJCJTlFJTIyJTdE&origin=intellList

3.3 安恒明御安全网关 远程代码执行漏洞

1) 漏洞描述

安恒 明御安全网关是一种网络安全产品，旨在提供可靠的网络安全防护和管理功能。

安恒 明御安全网关存在远程代码执行漏洞，导致攻击者可以直接执行系统

命令，从而控制目标系统。

攻击者可以利用远程代码执行漏洞，执行恶意代码或命令，并以系统权限执行操作，获取对目标系统的未经授权访问。

2) 爆发时间

2023 年 9 月 5 日

3) 影响版本

安恒 明御安全网关

4) 检测规则

检测流量中是否存在以下路径：

/webui/?g=aaa_portal_auth_config_reset

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.dbappsecurity.com.cn/product/cloud158.html

若无法进行升级的情况下，请使用该产品的用户进行如下操作：

1.配置防护设备以限制不可信 IP 对/webui/?g=aaa_portal_auth_config_reset 的请求：强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.tophant.com/detail/1698935642622398464?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNSVBRSU4OSVFNiU4MSU5MiVFNiU5OCU4RSVFNSVCRSVBMSVFNSVBRSU4OSVFNSU4NSVBOCVFNyVCRCU5MSVFNSU4NSVCMyUyMCVFOCVCRiU5QyVFNyVBOCU4QiVFNCVCQiVBMyVFNyVBMCU4MSVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNi

VCNCU5RSUyMiU3RA==&origin=intellList

3.4 绿盟 SAS 堡垒机 Exec 远程命令执行漏洞

1) 漏洞描述

绿盟 SAS 堡垒机 Exec 远程命令执行漏洞，漏洞存在于文件 ExecController.php 文件中

攻击者可利用该漏洞执行任意命令行。

2) 爆发时间

2023 年 9 月 8 日

3) 影响版本

SAS 堡垒机

4) 检测规则

检测流量中是否存在以下路径：

/webconf/Exec/index?cmd=

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

将 PHP 更新至 8.2.0 及以上版本

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1:在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.tophant.com/detail/1699967757329764352?keyword=

JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyVCQiVCRiVFNyU5QiU5RiUyMFNBUyVFNSVBMCVBMSVFNSU5RSU5MiVFNiU5QyVCQSUyMEV4ZWMlMjAlRTglQkYlOUMlRTclQTglOEIlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.5 深信服下一代防火墙 NGAF login.cgi 文件远程命令执行漏洞

1) 漏洞描述

深信服下一代防火墙是一款以应用安全需求出发而设计的下一代应用防火墙。深信服下一代防火墙在 login.cgi 路径下，PHPSESSID 处存在命令执行漏洞。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。

2) 爆发时间

2023 年 11 月 6 日

3) 影响版本

下一代防火墙 NGAF

4) 检测规则

检测流量中是否存在以下路径：

/cgi-bin/login.cgi

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.sangfor.com.cn/

若无法进行升级的情况下，请使用该产品的用户进行如下操作

过滤和验证用户输入： 对于 login.cgi 接口接收的用户参数，实施有效的输入过滤和验证。确保只接受符合预期格式和长度的输入，以防止攻击者利用恶意输入触发漏洞。

更新安全策略： 在 NGAF 设备上配置和更新安全策略，限制 login.cgi 接口的访问权限。仅允许授权用户或受信任的 IP 地址访问该接口。

网络层面的防护： 在网络层面配置防火墙规则，限制对 NGAF 设备的访问。仅允许必要的流量进入和离开，以减少攻击面。

监控登录活动： 加强对 NGAF 设备登录活动的监控，检测异常登录尝试和行为。实施实时或定期的日志审计，以及报警机制，及时发现潜在的安全问题。

审计用户权限： 审计和限制用户在 NGAF 设备上的权限。确保每个用户都只具有执行其工作所需的最小权限，以降低潜在攻击的影响范围。

VIP 平台链接：https://vip.tophant.com/detail/1721407503872430080?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCNyVCMSVFNCVCRiVBMSVFNiU5QyU4RCVFNCVCOCU4QiVFNCVCOCU4MCVFNCVCQiVBMyVFOSU5OCVCMiVFNyU4MSVBQiVFNSVBMiU5OSUyME5HQUYlMjBsb2dpbi5jZ2klMjAlRTYlOTYlODclRTQlQkIlQjYlRTglQkYlOUMlRTclQTglOEIlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklRTglRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.6 泛微 e-office welink 远程代码执行漏洞

1) 漏洞描述

泛微 e-office 是一款由泛微网络科技开发的协同管理平台，支持人力资源、财务、行政等多功能管理和移动办公。

泛微 e-office 远程代码执行漏洞是通过文件上传配合文件包含实现远程代码执行。

攻击者可以通过远程代码执行漏洞执行任意系统命令，从而完全控制受感染的系统。

2) 爆发时间

2023 年 10 月 18 日

3) 影响版本

e-office < 10.0_20230821

4) 检测规则

检测流量中是否存在以下路径：

/eoffice10/server/public/api/welink/welink-move

同时检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.e-office.cn/

若无法进行升级的情况下，请使用该产品的用户通过网络 ACL 策略限制访问来源，例如只允许来自特定 IP 地址或地址段的访问请求。

VIP 平台链接：https://vip.tophant.com/detail/1714580462783041536?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRSUyMGUtb2ZmaWNlJTIwd2VsaW5rJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.7 蓝凌 OA datajson 命令执行

1) 漏洞描述

蓝凌智能 OA 是由深圳市蓝凌软件股份有限公司开发，是一款针对中小企业的移动化智能办公产品 ，融合了钉钉数字化能力与蓝凌多年 OA 产品与服务经验，能全面满足企业日常办公在线、企业文化在线、客户管理在线、人事服务在

线、行政务服务在线等需求。

由于应用程序对传入命令的参数过滤不严导致恶意攻击值能控制最终执行的命令，进而入侵系统，造成严重破坏的高危漏洞。

2) 爆发时间

2023 年 10 月 12 日

3) 影响版本

蓝凌 OA

4) 检测规则

检测流量中是否存在以下路径：

/data/sys-common/datajson.js?s_bean=sysFormulaSimulateByJS&script=1112*112

同时检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://www.landray.com.cn

若无法进行升级的情况下，请使用该产品的用户仅允许可信 IP 访问 /data/sys-common/datajson.js 路由

VIP 平台链接：https://vip.tophant.com/detail/17123076295330406 40?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOCU5MyU5RCVFNSU4NyU4Q09BJTIwZGF0YWpzb24lMjAlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlMjIlN0Q=&origin=intellList

3.8 通达 OA getdata 远程命令执行漏洞

1) 漏洞描述

通达 OA 是一款协同办公软件，它可以帮助企业实现信息化管理，提高工作效率和协作能力。

通达 OA v11.9 getdata 接口存在任意命令执行漏洞，攻击者通过漏洞可以执行服务器任意命令控制服务器权限。

1、攻击者可以在受影响的应用程序上执行任意系统命令，这可能导致服务器或系统被完全控制。

2、攻击者可以执行命令来获取应用程序或系统中的敏感数据，例如数据库凭据、用户身份信息等。

2) 爆发时间

2023 年 9 月 12 日

3) 影响版本

通达 OA v11.9

通达 OA v11.10

4) 检测规则

检测流量中是否存在以下路径：

/general/appbuilder/web/portal/gateway/getdata?activeTab=%E5%27%19,1%3D%3Eeval(base64_decode(%22ZWNobyB2dWxuX3R4dDs=%22)))%3B/*&id=19&module=Carouselimage

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快升级至最新版本，下载地址如下：https://www.tongda2000.com

若无法进行升级的情况下，请使用该产品的用户进行如下操作 1、仅允许可信 ip 访问 /general/appbuilder/web/portal/gateway/getdata 路由

VIP 平台链接：https://vip.tophant.com/detail/1701513274593513472?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4MCU5QSVFOCVCRSVCRU9BJTIwZ2V0ZGF0YSUyMCVFOCVCRiU5QyVFNyVBOCU4QiVFNSU5MSVCRCVFNCVCQiVBNCVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.9 DedeCMS 文件上传漏洞(CVE-2023-36298)

1) 漏洞描述

Dedecms 是一款由上海卓卓网络科技有限公司研发的国产 PHP 网站内容管理系统，它可以让用户轻松地创建和管理各种类型的网站，如门户、企业、政府等，它具有强大的模板引擎、自定义模型、动静态部署、SEO 优化等功能。

DedeCMS 在 5.7.109 及之前版本存在文件上传漏洞。经过身份认证的攻击者利用系统的过滤缺陷可以上传恶意 Webshell 文件，从而控制服务器。

2) 爆发时间

2023 年 8 月 3 日

3) 影响版本

DedeCMS <= 5.7.109

4) 检测规则

检测流量中是否存在以下路径：

/dede/file

并检测上传文件名后缀和文件内容的类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

下载地址：https://www.dedecms.com/download

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1. 使用 WAF 防火墙等安全设备对服务器进行防护，对用户输入进行过滤，防止攻击者进行恶意利用。

VIP 平台链接：https://vip.tophant.com/detail/1687161866494808064?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkRlZGVDTVMlMjAlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUoQ1ZFLTIwMjMtMzYyOTgpJTIyJTdE&origin=intellList

3.10泛微 OA E-Office uploadify 任意文件上传漏洞

1) 漏洞描述

泛微 E-Office 是一个专业的协同 OA 办公软件，让中小型组织可以高效、便捷、安全地管理和协调各项业务。

泛微 E-Office 存在文件上传漏洞，攻击者可以通过 /inc/jquery/uploadify/uploadify.php 文件上传恶意文件，从而获取服务器权限，控制服务器。

2) 爆发时间

2023 年 8 月 30 日

3) 影响版本

Wevar E-Office 10

4) 检测规则

检测流量中是否存在以下路径：

/inc/jquery/uploadify/uploadify.php

同时检测上传文件的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用该产品的用户尽快联系厂商更新至安全版本。下载链接如下：https://www.e-office.cn/

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、在边界安全设备添加 PS、WAF 阻断规则，同时加强文件上传检测规则

2、内部对系统进行加固，对注入接口 incjquery/uploadify/uploadifyphp 进行参数过滤，阻断攻击特征。

VIP 平台链接：https://vip.tophant.com/detail/1696724541897838592?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRU9BJTIwRS1PZmZpY2UlMjB1cGxvYWRpZnklMjAlRTQlQkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.11泛微 OA Ecology upload_file.php 文件上传漏洞

1) 漏洞描述

泛微 Ecology9 是泛微科技公司推出的一款企业级数字化协同平台。该平台集成了企业常见的办公应用，如电子邮件、日历、通讯录、文档管理等，提供统一的界面和工作流程，帮助提高办公效率，旨在帮助企业实现信息化管理和协同办公。

泛微 OA 存在文件上传漏洞，可以上传 Webshell 到服务器并进行访问，从而造成服务器沦陷。

1. 上传恶意脚本文件到服务器中，通过访问该恶意文件从而执行文件中的恶意代码。

2. 攻击者可利用目录跳转上传 php、config 等文件，覆盖原有的系统文件，

到达篡改系统文件、甚至获取系统权限的目的。

3. 攻击者可上传 html、shtm 等文件，并写入非法博彩、赌博等恶意 SEO 页面或者写入恶意 js 文件进行钓鱼来非法获取用户信息等。

2) 爆发时间

2023 年 10 月 13 日

3) 影响版本

宏景 eHR

4) 检测规则

检测流量中是否存在以下路径：

/Upload/upload_file.php?l=

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快更新至最新的版本，下载链接如下：https://www.weaver.com.cn/cs/securityDownload.html#

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1：配置 URL 访问控制策略

2：对 OA 服务器上的网站后门文件进行及时查杀

VIP 平台链接：https://vip.tophant.com/detail/1712737705152090112?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRU9BJTIwRWNvbG9neSUyMHVwbG9hZF9maWxlLnBocCUyMCVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCVFNiVCNyVCQyU4RiVFNiVCNCVCQyVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.12金蝶 EAS uploadLogo.action 接口文件上传漏洞

1) 漏洞描述

金蝶 EAS 及 EAS Cloud 是金蝶软件公司推出的一套企业级应用软件套件，旨在帮助企业实现全面的管理和业务流程优化。金蝶 EAS 及 EAS Cloud 在 uploadLogo.action 存在文件上传漏洞，攻击者可以利用文件上传漏洞执行恶意代码、写入后门、读取敏感文件，从而可能导致服务器受到攻击并被控制。

金蝶 EAS 及 EAS Cloud 在 uploadLogo.action 存在文件上传漏洞，攻击者可以利用文件上传漏洞执行恶意代码、写入后门、读取敏感文件，从而可能导致服务器受到攻击并被控制。

2) 爆发时间

2023 年 11 月 3 日

3) 影响版本

金蝶 EAS

4) 检测规则

检测流量中是否存在以下路径：

/plt_portal/setting/uploadLogo.action

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请用户尽快升级至最新版本，下载地址如下：https://www.kingdee.com/products/eascloud.html

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、对上传文件类型进行验证，除在前端验证外在后端依然要做验证，后端可以进行扩展名检测，重命名文件，MIME 类型检测

以及限制上传文件的大小等限制来防御，或是将上传的文件其他文件存储服务器中。

2、严格限制和校验上传的文件，禁止上传恶意代码的文件。同时限制相关上传文件目录的执行权限，防止木马执行。

3、对上传文件格式进行严格校验，防止上传恶意脚本文件。

4、严格限制上传的文件路径

5、文件扩展名服务端白名单校验

6、文件内容服务端白名单校验。

7、上传文件重命名。

8、隐藏上传文件路径

VIP 平台链接：https://vip.tophant.com/detail/1720316476952547328?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4NyU5MSVFOCU5RCVCNiUyMEVBUyUyMHVwbG9hZExvZ28uYWN0aW9uJTIwJUU2JThFJUE1JUU1JThGJUEzJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJThGJUU0JUJBJTlFJTIyJTdE&origin=intellList

3.13用友 U8 Cloud upload.jsp 文件上传漏洞

6) 漏洞描述

用友网络科技股份有限公司

用友 U8 cloud 是用友开发的一款云 ERP。用友 U8 upload.jsp 存在任意文件上传漏洞，攻击者可利用该漏洞获取服务器权限。

攻击者可通过该漏洞在服务器端上传任意文件，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。

7) 爆发时间

2023 年 10 月 26 日

8) 影响版本

用友 U8 Cloud

9) 检测规则

检测流量中是否存在以下路径：

/linux/pages/upload.jsp

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

10) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本

官网链接：https://www.yonyou.com/

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、通过防火墙等安全设备设置访问策略，设置白名单访问。2、如非必要，禁止公网访问该系统。

VIP 平台链接：https://vip.tophant.com/detail/1717429090660782080?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QiUyMFU4JTIwQ2xvdWQlMjB1cGxvYWQuanNwJTIwJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJUThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.14用友 NC Cloud uploadChunk 任意文件上传漏洞

11) 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，基于云原生架构，打造开放、互联、融合、智能的一体化云平台，聚焦数智化管理、数智化经营、数智化商业等三大企业数智化转型战略方向，提供涵盖数字营销、财务共享、全球司库、智能制造、敏捷供应链、人才管理、智慧协同等 18 大解

决方案，帮助大型企业落地数智化。

用友 NC Cloud 的 uploadChunk 接口（/ncchr/pm/fb/attachment/uploadChunk）没有对用户上传的文件进行限制，导致经过身份验证的远程攻击者可上传任意文件，从而远程执行任意命令，获取服务器权限。

12) 爆发时间

2023 年 11 月 14 日

13) 影响版本

用友 NC Cloud

14) 检测规则

检测流量中是否存在以下路径：

/ncchr/pm/fb/attachment/uploadChunk?fileGuid=

并检测上传的文件名后缀和文件内容类型

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

15) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://dsp.yonyou.com/patchcenter/patchdetail/1022167047042645042 4/0/2

若无法进行升级的情况下，请使用该产品的用户进行如下操作

1、将上传目录和上传文件设置为不可执行，杜绝脚本执行。同时应保证服务器安全，避免文件解析漏洞。

2、使用白名单控制上传文件类型，只允许指定扩展名的文件上传。对上传文件后缀与 MIME Type 进行匹配校验，对文件头信息与文件后缀进行匹配校验。对单个文件大小和总文件数进行限制，避免拒绝服务攻击。对文件名进行输入校验，显示时进行输出编码。

3、上传文件应保存在指定路径下。对上传文件进行随机数重命名，避免文

件被覆盖。设置上传文件路径，使用户不能轻易访问自己上传的文件。文件应尽量保存在内容服务器或 web 目录外部，避免通过 web 应用直接访问上传的文件。

VIP 平台链接：https://vip.tophant.com/detail/1724304766491824128?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QiUyME5DJTIwQ2xvdWQlMjB1cGxvYWRDaHVuayUyMCVFNCVCQiVCQiVFNiU4NCU4RiVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.15金蝶云星空反序列化远程代码执行漏洞

1) 漏洞描述

由于金蝶云星空管理中心在处理序列化数据时，未对数据进行签名或校验，攻击手可以写入包含恶意代码的序列化数据，系统在进行反序列化时造成远程命令执行

攻击手可以写入包含恶意代码的序列化数据，系统在进行反序列化时造成远程命令执行

2) 爆发时间

2023 年 9 月 5 日

3) 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

4) 检测规则

检测流量中是否存在以下路径：

/Kingdee.BOS.ServiceFacade.ServicesStub.User.UserService.SaveUserPassport.common.kdsvc

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快更新安全补丁。

官方下载地址：https://www.kingdee.com/

若无法进行升级的情况下，请使用该产品的用户进行如下操作：

1.配置防护设备以限制不可信 IP 对该资源的请求：强烈建议在网络架构中部署防护设备，例如防火墙或 Web 应用程序防火墙（WAF），以限制来自不可信 IP 地址的请求。通过配置这些设备，可以过滤和阻止潜在的恶意流量，提高系统的安全性。此举可帮助防范诸如恶意请求、拒绝服务攻击等安全威胁。

VIP 平台链接：https://vip.tophant.com/detail/1698953452278910976?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4NyU5MSVFOCU5RCVCNiVFNCVCQSU5MSVFNiU5OCU5RiVFNyVBOSVCQSVFNSU4RiU4RCVFNSVCQSU4RiVFNSU4OCU5NyVFNSU4QyU5NiVFOCVCRiU5QyVFNyVBOCU4QiVFNCVCQiVBMyVFNyVBMCU4MSVFNiU4OSVBNyVFOCVBMSU4QyVFNiU4QyU4MSU4RiVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.16畅捷通 T+ 反序列化漏洞

1) 漏洞描述

用畅捷通 T+ 是一款基于互联网的新型企业管理软件。

畅捷通 T+ 存在.net 反序列化漏洞，未经过身份认证的攻击者可以通过构造恶意的序列化请求在目标服务器上执行任意命令。

攻击者可以通过反序列化漏洞，将恶意的序列化数据传递给目标应用程序，从而导致执行非预期的代码。这可能会使攻击者能够在受影响的系统上执行任意的代码，甚至获取对系统的完全控制。

2) 爆发时间

2023 年 9 月 7 日

3) 影响版本

畅捷通 T+ 13.0

畅捷通 T+ 16.0

4) 检测规则

检测流量中是否存在以下路径：

/tplus/ajaxpro/Ufida.T.CodeBehind._PriorityLevel,App_Code.ashx?method=

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

请使用此产品的用户尽快打补丁或更新到最新版本：https://sem.chanjet.com/

若无法进行升级的情况下，请使用该产品的用户进行如下操作 1、仅允许可信 ip 访问 /tplus/ajaxpro/Ufida.T.CodeBehind._PriorityLevel,App_Code.ashx 路由

VIP 平台链接：https://vip.tophant.com/detail/1699702166140358656?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NSU4NSVFNiU4RCVCNyVFOSU4MCU5QVQlMkIlMjAlRTUlOEYlOEQlRTUlQkElOEYlRTUlODglOTclRTUlOEMlOTYlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList