斗象科技
TOPHANT

2024-06

2024
HW 必修高危漏洞集合

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

版本：v1.0

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 2024 年 3 月份至 2024 年 5 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

2024HW 必修高危漏洞集合持续更新中，请持续关注。

二、 漏洞汇总数据

本文档为斗象发布的《2024HW 必修高危漏洞集合_1.0》对自 2024 年 3 月以来截止到目前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：6 个

  涉及厂商：YzmCMS、畅捷通、pgAdmin、泛微、锐捷、奇安信、

- 文件上传

  漏洞数量：6 个

  涉及厂商：泛微、用友、致远、奇安信

- 不安全的反序列化

  漏洞数量：3 个

  涉及厂商：畅捷通、用友、金蝶

- 其他

  漏洞数量：2

  漏洞类型：命令执行，JNDI 注入

  涉及厂商：金山、用友

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
YzmCMS pay_callback.html 远程代码执行漏洞	远程代码执行	YzmCMS	YzmCMS
畅捷通 T+ App_Code.ashx 远程命令执行漏洞	远程命令执行	畅捷通	畅捷通 T+
pgAdmin 远程代码执行漏洞	远程代码执行	pgAdmin	pgAdmin <= 6.16

泛微 E-Office10 atuh-file 远程代码执行漏洞	远程代码执行漏洞	泛微	v10.0_20180516 < E-Office10 < v10.0_20240222
锐捷 EWEB auth 远程代码执行漏洞	远程代码执行漏洞	锐捷	锐捷 EWEB
网神 SecGate 3600 防火墙 sysToolsDetectNet.cgi 远程代码执行漏洞	远程代码执行漏洞	奇安信	网神 SecGate3600 防火墙
泛微 OA e-office webservice 任意文件上传漏洞	任意文件上传	泛微	泛微 OA e-office
用友-U8-CRM swfupload 文件上传漏洞	任意文件上传	用友	用友-U8-CRM
泛微 E-Office mobile_upload_save 任意文件上传漏洞	任意文件上传	泛微	泛微 E-Office 9.5
致远互联 OA fileUpload.do 文件上传漏洞	任意文件上传	致远	致远 A8 V5.x 致远 A6 V5.x 致远 A8N 致远 G6 致远 G6N
网神 SecGate3600 防火墙 import_save 任意文件上传漏洞	任意文件上传	奇安信	网神 SecGate3600 防火墙
用友 NC-Cloud doPost 任意文件上传漏洞	任意文件上传	用友	用友 NC-Cloud
用友 GRP-U8	不安全的反	用友	用友 GRP-U8

VerifyToken 反序列化漏洞	序列化		
畅捷通 T+ Ufida.T.DI.UIP.RRA.RRATableController 反序列化漏洞	不安全的反序列化	畅捷通	畅捷通 T+
金蝶云星空 ServiceGateway.GetServiceUri.common 反序列化	不安全的反序列化	金蝶	金蝶云星空
金山 V8 终端安全系统 pdf_maker.php 命令执行漏洞	命令执行	金山	金山 V8 终端安全系统
用友 NC-Cloud PMCloudDriveProjectStateServlet JNDI 注入漏洞	JNDI 注入漏洞	用友	用友 NC-Cloud

三、 自查高危详情

3.1 YzmCMS pay_callback.html 远程代码执行漏洞

1) 漏洞描述

YzmCMS 采用面向对象方式自主研发的 YZMPHP 框架开发，它是一款开源高效的内容管理系统，产品基于 PHP+Mysql 架构，可运行在 Linux、Windows、MacOSX、Solaris 等各种平台上。

YzmCMS 存在远程代码执行漏洞，未经身份验证的远程攻击者可利用此漏洞执行任意系统命令。

2) 披露时间

2024 年 5 月 6 日

3) 影响版本

YzmCMS

4) 检测规则

检测流量中是否存在以下路径：/pay/index/pay_callback.html

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复程序，请使用此产品的用户尽快更新至安全版本：

Zoho ManageEngine ServiceDesk Plus >= 11306

官方下载地址：https://www.yzmcms.com

VIP 平台链接：https://vip.vulbox.com/detail/1787360451298988032?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMll6bUNNUyUyMHBheV9jYWxsYmFjay5odG1sJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJ

DJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.2 畅捷通 T+ App_Code.ashx 远程命令执行漏洞

1) 漏洞描述

畅捷通 T+专属云适用于需要一体化管理的企业，财务管理、业务管理、零售管理、生产管理、物流管理、移动仓管、营销管理、委外加工等人财货客一体化管理。

在畅捷通 T+ App_Code.ashx 存在远程命令执行漏洞，未授权攻击者可以利用此漏洞执行系统命令，并获取服务器权限。

2) 爆发时间

2024 年 4 月 9 日

3) 影响版本

畅捷通 T+

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

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。下载地址如下：https://www.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

仅允许可信 ip 访问 /tplus/ajaxpro/Ufida.T.CodeBehind._PriorityLevel,App_Cod

e.ashx 路由

VIP 平台链接：https://vip.vulbox.com/detail/1777523639692955648?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NSU4NSVFNiU4RCVCNyVFOSU4MCU5QVQlMkIlMjBBcHBfQ29kZS5hc2h4JTIwJUU4JUJGJTlDJUU3JUE4JThCJUU1JTkxJUJEJUU0JUJCJUE0JUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.3 pgAdmin 远程代码执行漏洞(CVE-2022-4223)

1) 漏洞描述

pgAdmin 是一个著名的 PostgreSQL 数据库管理平台。

pgAdmin 包含一个 HTTP API 可以用来让用户选择并验证额外的 PostgreSQL 套件，比如 pg_dump 和 pg_restore。但在其 6.16 版本及之前，用户对于创建的路径没有做合适的验证，导致未授权的用户可以在目标服务器上执行任意命令。

2) 爆发时间

2024 年 4 月 7 日

3) 影响版本

pgAdmin <= 6.16

4) 检测规则

检测流量中是否存在以下路径：

/misc/validate_binary_path

并且请求正文中，是否有“jndiName”参数

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.kingdee.com

VIP 平台链接 https://vip.vulbox.com/detail/1776855870139928576?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMnBnQWRtaW4lMjAlRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUoQ1ZFLTIwMjItNDIyMyklMjIlN0Q=&origin=intellList&source=vb

3.4 泛微 E-Office10 atuh-file 远程代码执行漏洞

1) 漏洞描述

泛微 e-office10 是一款专业的协同 OA 软件，支持全终端，移动功能显著，包括知识文档管理、流程管理、项目管理、客户管理、费用管理、协作区、任务管理等功能模块。

泛微 e-office10 在 10.0_20240222 版本之前存在远程代码执行漏洞。未经授权的攻击者可以构造特制的请求包进行利用，从而进行任意代码执行，控制服务器。

2) 爆发时间

2024 年 3 月 28 日

3) 影响版本

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

4) 检测规则

检测流量中是否存在以下路径：

/eoffice10/server/public/api/attachment/atuh-file

/eoffice10/server/public/api/attachment/path/migrate

/eoffice10/server/public/api/empower/import

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更新至安全版本。

版本号：E-Office10 >= v10.0_20240222

版本链接：https://service.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

仅允许可信 ip 访问 /eoffice10/server/public/api/attachment/atuh-file 路由

VIP 平台链接：https://vip.vulbox.com/detail/1773229647547469824?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRUUtT2ZmaWNlMTAlMjBhdHVoLWZpbGUlMjAlRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList&source=vb

3.5 锐捷 EWEB auth 远程代码执行漏洞

1) 漏洞描述

锐捷睿易是锐捷网络针对商业市场的子品牌。拥有易网络、交换机、路由器、无线、安全、云服务六大产品线，解决方案涵盖商贸零售、酒店、KTV、网吧、监控安防、物流仓储、制造业、中小教育、中小医疗、中小政府等商业用户。

锐捷 EWEB auth 接口存在远程代码执行漏洞，未授权的攻击者可以通过该漏洞执行恶意命令，进而导致服务器失陷。

2) 爆发时间

2024 年 3 月 25 日

3) 影响版本

锐捷 EWEB

4) 检测规则

检测流量中是否存在以下路径：

/cgi-bin/luci/api/auth

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版本，下载地址如下 https://www.ruijie.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

仅允许可信 ip 访问 /cgi-bin/luci/api/auth 路由

VIP 平台链接：https://vip.vulbox.com/detail/1772168762427052032?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU5NCU5MCVFNiU4RCVCNyUyMEVXRUIlMjBhdXRoJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJUFBJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.6 网神 SecGate 3600 防火墙 sysToolsDetectNet.cgi 远程代码执行漏洞

1) 漏洞描述

网神 SecGate3600 防火墙是一款高性能的下一代防火墙，它可以提供防火墙、VPN、IPS、内容过滤、带宽管理、用户认证等多项安全技术，以及与奇虎 360 公司的情报威胁、终端协同、木马云、病毒云、URL 云等智能联动功能。

网神 SecGate 3600 防火墙 sysToolsDetectNet.cgi 接口 存在远程代码执行漏洞。未授权的攻击者可以通过该漏洞远程执行代码，从而获取大量敏感信息，甚

至控制服务器。

2) 爆发时间

2024 年 3 月 19 日

3) 影响版本

网神 SecGate3600 防火墙

4) 检测规则

检测流量中是否存在以下路径：

/cgi-bin/sysTools/sysToolsDetectNet.cgi

并且请求正文中是否存在“targetHost” 参数

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复程序，请使用此产品的用户尽快更新至安全版本：

官方下载地址：https://www.legendsec.com/newsec.php?up=2&cid=215

VIP 平台链接：https://vip.vulbox.com/detail/1769907947934191616?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyVCRCU5MSVFNyVBNSU5RVNlY0dhdGUlMjAzNjAwJUU5JTk4JUIyJUU3JTgxJUFCJUU1JUEyJTk5JTIwc3lzVG9vbHNEZXRlY3ROZXQuY2dpJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJTkwJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.7 泛微 OA e-office webservice 任意文件上传漏洞

1) 漏洞描述

泛微 e-office 是泛微旗下的一款标准协同移动办公平台。主要面向中小企业,平台全方位覆盖日常办公场景,可以有效提升组织管理与协同效率。

泛微 e-office /webservice/upload/upload.php 接口存在任意文件上传漏洞。未收取的攻击者可以通过该漏洞上传恶意脚本文件，从而控制服务器。

2) 爆发时间

2024 年 4 月 25 日

3) 影响版本

泛微 e-office

4) 检测规则

检测流量中是否存在以下路径：

/webservice/upload/upload.php

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.weaver.com.cn

VIP 平台链接：https://vip.vulbox.com/detail/1783324050983096320?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRU9BJTIwZS1vZmZpY2UlMjB3ZWJzZXJ2aWNlJTIwJUU0JUJCJUJCJUU2JTg0JThGJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.8 用友-U8-CRM swfupload 文件上传漏洞

1) 漏洞描述

用友 U8-CRM 是一款由用友软件开反的各尸大系信理低了 M 兹 Eh 能，包括客户信息管理、销售机会跟踪、市场营销活帮助企业有效管理和维护与客户之间的关系。该系统提供了一系列功能，包

动管理、客户服务支持等。通过使用用友 U8-CRM，企业可以更好地了解客户需求，提高销售效率，增强客户满意度，并实现更好的客户关系管理。

用友 U8-CRM swfupload 接口存在任意文件上传漏洞。该漏洞使得攻击者可以在受影响的系统上上传恶意文件，潜在风险包括远程执行恶意代码、访问敏感数据，以及其他危险操作。攻击者可以通过上传恶意文件来滥用系统，可能导致灾难性后果。

2) 爆发时间

2024 年 4 月 22 日

3) 影响版本

用友 U8-CRM

4) 检测规则

检测流量中是否存在以下路径：

/ajax/swfupload.php?DontCheckLogin

并同时检测上传的文件名和文件内容类型

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

请用户尽快升级至最新版本，下载地址如下：https://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

仅允许可信 ip 访问/ajax/swfupload.php?DontCheckLogin=1&vname=file 路由

VIP 平台链接：https://vip.vulbox.com/detail/1782242773613809664?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4Qi1VOC1DUk0lMjBzd2Z1cGxvYWQlMjAlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList&source=vb

3.9 泛微 E-Office mobile_upload_save 任意文件上传漏洞

1) 漏洞描述

泛微 E-Office 是中国泛微科技（Weaver）公司的一个协同办公系统。

泛微 E-Office 9.5 版本存在代码问题漏洞，该漏洞源于 App/Ajax/ajax.php?action=mobile_upload_save 存在未知函数，通过参数 upload_quwan 导致不受限制的上传。未经身份验证的远程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

2024 年 4 月 18 日

3) 影响版本

泛微 E-Office 9.5

4) 检测规则

检测流量中是否存在以下路径：

/E-mobile/App/Ajax/ajax.php

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.e-office.cn/

VIP 平台链接：https://vip.vulbox.com/detail/1780789293653037056?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRUUtT2ZmaWNlJTIwbW9iaWxlX3VwbG9hZF9zYXZlJTIwJUU0JUJCJUJCJUU2JTg0JThGJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.10致远互联 OA fileUpload.do 文件上传漏洞

1) 漏洞描述

致远互联-OA 是数字化构建企业数字化协同运营中台，面向企业各种业务场景提供一站式大数据分析解决方案的协同办公软件。

在致远互联-OA 接口 fileUpload.do 接口处存在文件上传漏洞，未经身份验证的远程攻击者可通过目录遍历的方式绕过上传接口限制，并利用 menu.do 接口替换上传文件的 fileid 值实现 webshell 上传到服务器，获取服务器权限。

2) 爆发时间

2024 年 4 月 9 日

3) 影响版本

致远 A8 V5.x

致远 A6 V5.x

致远 A8N

致远 G6

致远 G6N

4) 检测规则

检测流量中是否存在以下路径：

/seeyon/autoinstall.do/../../seeyon/fileUpload.do

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.seeyon.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

仅允许可信 ip 访问 /seeyon/autoinstall.do 路由

VIP 平台链接：https://vip.vulbox.com/detail/1777531876387459072?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOCU4NyVCNCVFOCVCRiU5QyVFNCVCQSU5MiVFOCU4MSU5NE9BJTIwZmlsZVVwbG9hZC5kbyUyMCVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyU4MCVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList&source=vb

3.11网神 SecGate3600 防火墙 import_save 任意文件上传漏洞

1) 漏洞描述

网神 SecGate3600 防火墙是一款高性能的下一代防火墙，它可以提供防火墙、VPN、IPS、内容过滤、带宽管理、用户认证等多项安全技术，以及与奇虎360 公司的情报威胁、终端协同、木马云、病毒云、URL 云等智能联动功能。

网神 SecGate3600 防火墙存在任意文件上传漏洞。未授权的攻击者可以通过该漏洞上传任意文件，从而控制服务器

2) 爆发时间

2024 年 3 月 8 日

3) 影响版本

网神 SecGate3600 防火墙

4) 检测规则

检测流量中是否存在以下路径：

/?g=app

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.legendsec.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

不要将该设备设置为公网开放，防止未知来源的 IP 对其进行恶意利用。

VIP 平台链接：https://vip.vulbox.com/detail/1765985770969108480?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyVCRCU5MSVFNyVBNSU5RVNlY0

dhdGUzNjAwJUU5JTk4JUIyJUU3JTgxJUFCJUU1JUEyJTk5JTIwaW1wb3J0X3NhdmUlMjAlRTQlQkIlQkIlRTYlODQlOEYlRTYlOTYlODclRTQlQkIlQjYlRTQlQjglOEElRTQlQkMlQTAlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList&source=vb

3.12用友 NC-Cloud doPost 任意文件上传漏洞

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，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，帮助大型企业全面落地数智化。

用友 NC-Cloud doPost 接口存在任意文件上传漏洞，未授权的攻击者可以通过该漏洞上传恶意的脚本文件，从而控制服务器。

2) 爆发时间

2024 年 3 月 26 日

3) 影响版本

用友 NC-Cloud

4) 检测规则

检测流量中是否存在以下路径：

/portal/pt/servlet/saveXmlToFileServlet/doPost

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://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

仅允许可信 ip 访问 /portal/pt/servlet/saveXmlToFileServlet/doPost 路由

VIP 平台链接：https://vip.vulbox.com/detail/17724492061586268 16?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4Qk5DLUNsb3VkJTIwZG9Qb3N0JTIwJUU0JUJCJUJCJUU2JTg0JThGJUU2JTk2JTg3JUU0JUJCJUI2JUU0JUI4JThBJUU0JUJDJUEwJUU2JUJDJDThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.13用友 GRP-U8 VerifyToken 反序列化漏洞

6) 漏洞描述

用友 GRP-U8 是一款功能全面的会计软件，适用于企业的财务管理需求。它提供了财务核算、财务分析、资产管理等全面的财务管理功能，实现了会计凭证自动生成、科目余额表生成等功能，大大简化了手动处理的繁琐过程。此外，该软件还具备数据备份、恢复等安全措施，确保企业财务数据的安全性。

用友 GRP-U8 R10 系列版本存在反序列化漏洞，未经身份验证的攻击者可利用此漏洞获取服务器权限。

7) 爆发时间

2024 年 4 月 25 日

8) 影响版本

用友 GRP-U8 R10 系列版本

9) 检测规则

检测流量中是否存在以下路径：

/VerifyToken

请求正文中是否包含“PARAM”参数

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：https://www.yonyou.com

VIP 平台链接：https://vip.vulbox.com/detail/1783392218787221504?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4QkdSUC1VOCUyMFZlcmlmeVRva2VuJTIwJUU1JThGJThEJUU1JUJBJThGJUU1JTg4JTk3JUU1JThDJTk2JUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.14畅捷通 T+ Ufida.T.DI.UIP.RRA.RRATableController 反序列化漏洞

11) 漏洞描述

畅捷通 T+是一款企业管理软件，主要面向中小企业。它提供了包括财务、采购、销售、库存、生产制造、人力资源等在内的全面企业管理解决方案。通过畅捷通 T+，企业可以实现对业务流程的数字化管理，提高工作效率，降低成本，增强企业竞争力。

畅捷通 T+ /tplus/ajaxpro/Ufida.T.DI.UIP.RRA.RRATableController,Ufida.T.DI.UIP.ashx 接口存在.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。

12) 爆发时间

2024 年 3 月 19 日

13) 影响版本

畅捷通 T+

14) 检测规则

检测流量中是否存在以下路径：

/tplus/ajaxpro/Ufida.T.DI.UIP.RRA.RRATableController,Ufida.T.DI.UIP.ashx?method=GetStoreWarehouseByStore

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://www.chanjet.com

VIP 平台链接：https://vip.vulbox.com/detail/1769992957022310400?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NSU4NSVFNiU4RCVCNyVFOSU4MCU5QVQlMkIlMjBVZmlkYS5ULkRJLlVJUC5SUkEuUlJBVGFibGVDb250cm9sbGVyJTIwJUU1JThGJThEJUU1JUJBJThGJUU1JTg4JTk3JUU1JThDJTk2JUU2JUJDJThDJUI0JTlFJTIyJTdE&origin=intellList&source=vb

3.15金蝶云星空 ServiceGateway.GetServiceUri.common 反序列化

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

2) 爆发时间

2024 年 3 月 15 日

3) 影响版本

金蝶云星空

4) 检测规则

检测流量中是否存在以下路径：

/Kingdee.BOS.ServiceFacade.ServicesStub.ServiceGateway.GetServiceUri.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/

VIP 平台链接：https://vip.vulbox.com/detail/1768457004478763008?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4NyU5MSVFOCU5RCVCNiVFNCVCQSU5MSVFNiU5OCU5RiVFNyVBOSVCQSUyMFNlcnZpY2VHYXRld2F5LkdldFNlcnZpY2VVcmkuY29tbW9uJTIwJUU1JThGJThEJUU1JUJBJTg4JUU1JThGJTg2JUU1JTg4JTk2JUU1JThDJTk2JTIyJTdE&origin=intellList&source=vb

3.16金山 V8 终端安全系统 pdf_maker.php 命令执行漏洞

1) 漏洞描述

金山 V8 终端安全系统是一款集合了安全、管理、监控、指挥、响应和应急等一系列功能的集成终端安全解决方案。它采用了符合国际安全标准的可靠安全防御体系，能够为企业提供全面的终端安全管控。

金山 V8 终端安全系统 pdf_maker.php 存在命令执行漏洞，由于没有过滤危险字符，导致未授权的攻击者可以通过该漏洞构造特殊字符进行命令拼接执行任意命令

2) 爆发时间

2024 年 4 月 9 日

3) 影响版本

金山 V8 终端安全系统

4) 检测规则

检测流量中是否存在以下路径：

/inter/pdf_maker.php

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.ejinshan.ne

t/lywz/index

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

仅允许可信 ip 访问 /inter/pdf_maker.php 路由 VMware vCenter Server 6.5 系列 >= 6.5 U3n

VIP 平台链接：https://vip.vulbox.com/detail/17776150467556188 16?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOSU4NyU5MSVFNSVCMSVCMVY4JUU3JUJCJTg4JUU3JUFCJUFGJUU1JUFFJTg5JUU1JTg1JUE4JUU3JUIzJUJCJUU3JUJCJTlGJTIwcGRmX21ha2VyLnBocCUyMCVFNSU5MSVCRCVFNCVCQiVBNCVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList&source=vb

3.17用友 NC-Cloud PMCloudDriveProjectStateServlet JNDI 注入漏洞

1) 漏洞描述

用友 NC 是“企业资源规划（Enterprise Resource Planning）”的缩写，是指用友软件股份有限公司开发的一套企业管理软。用友 NC 系统是一种集成管理企业各项业务流程的信息化解决方案。该系统涵盖了财务、人力资源、供应链管理等多个方面，旨在帮助企业提高运营效率、优化资源利用、提升管理水平。用友 NC Cloud 系统 PMCloudDriveProjectStateServlet.class 接口 处存在 JNDI 注入漏洞，未经身份验证的攻击者可通过此漏洞可以在服务端执行任意命令，获取服务器权限。

2) 披露时间

2024 年 3 月 6 日

3) 影响版本

NCC2105、NCC2111、YonBIP 高级版 2207、YonBIP 高级版 2305

4) 检测规则

检测流量中是否存在以下路径：

/service/~pim/PMCloudDriveProjectStateServlet

以及请求正文中是否存在“data_source”参数

斗象智能安全 PRS 最新规则已支持检测，如有疑问可联系售后支持。

5) 修复方案

厂商已发布了漏洞修复程序，请使用此产品的用户尽快更新至安全版本：

官方下载地址：https://sem.chanjet.com/

VIP 平台链接：https://vip.vulbox.com/detail/17652596903186309 12?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NCVBOCVFNSU4RiU4Qk5DLUNsb3VkJTIwUE1DbG91ZERyaXZlUHJvamVjdFN0YXRlU2VydmxldCUyMEpOREklRTYlQjMlQTglRTUlODUlQTUlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList&source=vb