斗象科技
TOPHANT

2024 - 06

2024

HW必修高危漏洞集合

版本：V4.0

斗象科技 - 漏洞情报中心
EMAIL: SERVICE@TOPHANT.COM
TEL: 400-156-9866

目录 CONTENTS

1 前言 3

2 漏洞汇总数据 4

3 自查高危详情 9

3.1 APACHE NIFI H2 JDBC 远程代码执行漏洞(CVE-2023-34468) 9

3.2 MANAGEENGINE 多个产品 远程代码执行漏洞(CVE-2022-47966) 10

3.3 ADOBE COLDFUSION 远程代码执行漏洞(CVE-2023-26360) 12

3.4 瑞友天翼应用虚拟化系统 远程代码执行漏洞 13

3.5 APACHE SOLR 远程代码执行漏洞(CNVD-2023-27598) 15

3.6 APACHE DRUID 远程代码执行漏洞 16

3.7 POWERJOB 未授权远程代码执行漏洞(CVE-2023-29926) 17

3.8 DEDECMS 远程代码执行漏洞(CVE-2023-2928) 18

3.9 大华智慧园区综合管理平台 远程代码执行漏洞 20

3.10 SUGARCRM 远程代码执行漏洞(CVE-2023-22952) 21

3.11 WEBLOGIC 远程代码执行漏洞(CVE-2023-21839) 22

3.12 禅道项目管理系统 命令注入漏洞(CNVD-2023-02709) 24

3.13 TP-LINK ARCHER AX21 AX1800命令注入漏洞 （CVE-2023-1389） 25

3.14 VMWARE ARIA OPERATIONS FOR NETWORKS 命令注入漏洞(CVE-2023-20887) 26

3.15 APACHE SOLR 命令执行漏洞(CNVD-2023-34111) 28

3.16 NGINXWEBUI 远程命令执行漏洞 29

3.17 海康威视 IVMS-8700综合安防管理平台软件 文件上传漏洞 30

3.18 泛微E-COLOGY9协同办公系统 任意文件上传漏洞 32

3.19 大华智慧园区综合管理平台 文件上传漏洞(CVE-2023-3836) 33

3.20 泛微E-COLOGY9协同办公系统 SQL注入漏洞(CNVD-2023-12632) 34

3.21 畅捷通T+ SQL注入漏洞 36

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 1 月份至 2023 年 7 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。

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
第四期《2024HW 必修高危漏洞集合_4.0》收录 2023 年 1 月-2023 年 7 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_4.0》对自 2023 年 1 月至 2023 年 7 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：11 个

  涉及厂商：apache、ManageEngine、adobe、瑞友天翼、PowerJob、dede cms、大华股份、sugarcrm、oracle

- 命令注入

  漏洞数量：5 个

  涉及厂商：禅道、tp-link、vmware、apache、nginx、

- 任意文件上传

  漏洞数量：3 个

  涉及厂商：海康威视、weaver、dahuasecurity

- SQL 注入漏洞

  漏洞数量：2 个

  涉及厂商：weaver、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
Apache NiFi H2 JDBC 远程代码执行漏洞 (CVE-2023-34468)	远程代码执行漏洞	apache	0.0.2 <= Apache NiFi <= 1.21.0
ManageEngine 多个产品 远程代码执行漏洞 (CVE-2022-47966)	远程代码执行漏洞	ManageEngine	Access Manager Plus* <= 4307 Active Directory 360** <= 4309 ADAudit Plus** <= 7080

			ADManager Plus** <= 7161 ADSelfService Plus** <= 6210 Analytics Plus* <= 5140 Application Control Plus* <= 10.1.2220.17 Asset Explorer** <= 6982 Browser Security Plus* <= 11.1.2238.5 Device Control Plus* <= 10.1.2220.17 Endpoint Central* <= 10.1.2228.10 Endpoint Central MSP* <= 10.1.2228.10 Endpoint DLP* <= 10.1.2137.5 Key Manager Plus* <= 6400 OS Deployer* <= 1.1.2243.0 PAM 360* <= 5712 Password Manager Pro* <= 12123 Patch Manager Plus* <= 10.1.2220.17 Remote Access Plus* <= 10.1.2228.10

			Remote Monitoring and Management (RMM)* <= 10.1.40 ServiceDesk Plus** <= 14003 ServiceDesk Plus MSP** <= 13000 11017 <= SupportCenter Plus** <= 11025 Vulnerability Manager Plus* <= 10.1.2220.17
Adobe ColdFusion 远程代码执行漏洞 (CVE-2023-26360)	远程代码执行漏洞	adobe	ColdFusion 2018 <= Update 15 ColdFusion 2021 <= Update 5
瑞友天翼应用虚拟化系统 远程代码执行漏洞	远程代码执行漏洞	瑞友天翼	5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1
Apache Solr 远程代码执行漏洞 (CNVD-2023-27598)	远程代码执行漏洞	apache	8.10.0 <= Apache Solr < 9.2.0
Apache Druid 远程代码执行漏洞	远程代码执行漏洞	apache	Apache Druid <= 25.0.0
PowerJob 未授权远程代码执行漏洞 (CVE-2023-29926)	远程代码执行漏洞	PowerJob	PowerJob V4.3.2
DedeCMS 远程代码执行漏洞 (CVE-2023-2928)	远程代码执行漏洞	dedecms	DedeCMS <= 5.7.106

大华智慧园区综合管理平台 远程代码执行漏洞	远程代码执行漏洞	大华股份	大华智慧园区综合管理平台 <= V3.001.0000004.18.R.2223994
SugarCRM 远程代码执行漏洞 (CVE-2023-22952)	远程代码执行漏洞	sugarcrm	SugarCRM < 12.0.2 SugarCRM < 11.0.5
Weblogic 远程代码执行漏洞 (CVE-2023-21839)	远程代码执行漏洞	oracle	WebLogic_Server = 12.2.1.3.0 WebLogic_Server = 12.2.1.4.0 WebLogic_Server = 14.1.1.0.0
禅道项目管理系统 命令注入漏洞 (CNVD-2023-02709)	命令注入漏洞	禅道	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)
TP-Link Archer AX21 AX1800 命令注入漏洞（CVE-2023-1389）	命令注入漏洞	tp-link	TP-LINK TP-Link Archer AX21 < 1.1.4 Build 20230219
VMware Aria Operations for Networks 命令注入漏洞(CVE-2023-20887)	命令注入漏洞	vmware	VMware Aria Operations Networks 6.x

Apache Solr 命令执行漏洞 (CNVD-2023-34111)	命令注入漏洞	apache	Apache Solr <= 8.3.1
nginxWebUI 远程命令执行漏洞	命令注入漏洞	nginx	nginxWebUI <= 3.4.6
海康威视 iVMS-8700 综合安防管理平台软件 文件上传漏洞	任意文件上传漏洞	海康威视	海康威视 iVMS-8700 综合安防管理平台软件
泛微 e-cology9 协同办公系统 任意文件上传漏洞	任意文件上传漏洞	weaver	泛微 e-cology9 协同办公系统 < 10.58.3
大华智慧园区综合管理平台 文件上传漏洞 (CVE-2023-3836)	任意文件上传漏洞	dahuasecurity	大华智慧园区综合管理平台 <= 20230713 之前发行版本
泛微 e-cology9 协同办公系统 SQL 注入漏洞 (CNVD-2023-12632)	SQL 注入漏洞	weaver	泛微 e-cology9 协同办公系统 < 10.56
畅捷通 T+ SQL 注入漏洞	SQL 注入漏洞	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 Apache NiFi H2 JDBC 远程代码执行漏洞 (CVE-2023-34468)

1) 漏洞描述

Apache NiFi 是一个易于使用、强大、可靠的系统，用于处理和分发数据。它支持强大和可扩展的数据路由、转换和系统中介逻辑的有向图。

Apache NiFi 在 0.0.2-1.21.0 版本中存在远程代码执行漏洞。Apache NiFi 中的 DBCPConnectionPool 和 HikariCPConnectionPool 控制器服务允许经过认证和授权的用户用 H2 驱动配置数据库 URL，从而实现自定义代码执行。

2) 披露时间

2023 年 6 月 12 日

3) 影响版本

0.0.2 <= Apache NiFi <= 1.21.0

4) 检测规则

检测流量中是否存在以下路径：/nifi-api/process-groups/root

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://github.com/apache/nifi/tags

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：在默认配置中禁用 H2 JDBC URL

VIP 平台链接：https://vip.tophant.com/detail/1668317671621529600?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkFwYWNoZSUyME5pRmklMjBIMiUyMEpEQkMlMjAlRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUoQ1ZFLTIwMjMtMzQ0NjgpJTIyJTdE&origin=intellList

3.2 ManageEngine 多个产品 远程代码执行漏洞 (CVE-2022-47966)

1) 漏洞描述

ManageEngine 是专业研发和销售 IT 管理软件、网管软件的品牌。

ManageEngine 多个产品中存在远程代码执行漏洞，该漏洞是由于使用了一个古老的第三方依赖：Apache Santuario 所导致的。

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) 爆发时间

2023 年 1 月 17 日

3) 影响版本

Access Manager Plus* <= 4307

Active Directory 360** <= 4309

ADAudit Plus** <= 7080

ADManager Plus** <= 7161

ADSelfService Plus** <= 6210

Analytics Plus* <= 5140

Application Control Plus* <= 10.1.2220.17

Asset Explorer** <= 6982

Browser Security Plus* <= 11.1.2238.5

Device Control Plus* <= 10.1.2220.17

Endpoint Central* <= 10.1.2228.10

Endpoint Central MSP* <= 10.1.2228.10

Endpoint DLP* <= 10.1.2137.5

Key Manager Plus* <= 6400

OS Deployer* <= 1.1.2243.0

PAM 360* <= 5712

Password Manager Pro* <= 12123

Patch Manager Plus* <= 10.1.2220.17

Remote Access Plus* <= 10.1.2228.10

Remote Monitoring and Management (RMM)* <= 10.1.40

ServiceDesk Plus** <= 14003

ServiceDesk Plus MSP** <= 13000

11017 <= SupportCenter Plus** <= 11025

Vulnerability Manager Plus* <= 10.1.2220.17

4) 检测规则

检测流量中是否存在以下路径：/SamlResponseServlet

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.manageengine.com/security/advisory/CVE/cve-2022-47966.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、限制对受影响的 ManageEngine 产品的访问。确保只有授权人员可以访问管理界面，通过强密码、访问控制列表（ACL）或其他安全措施来阻止未经授权的访问。

2、使用网络监控工具实时监控受影响的 ManageEngine 产品的网络流量和活动。这有助于及时发现潜在的攻击行为，并采取相应的应对措施。

VIP 平台链接：https://vip.tophant.com/detail/1615274932701368320?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMk1hbmFnZUVuZ2luZSUyMCVFNSVBNCU5QSVFNCVCOCVBQSVFNCVCQSVBNyVFNSU5MyU4MSUyMCVFOCVCRiU5QyVFNyVBOCU4QiVFNCVCQiVBMyVFNyVBMCU4MSVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCNCU5RShDVkUtMjAyMi00Nzk2NiklMjIlN0Q=&origin=intellList

3.3 Adobe ColdFusion 远程代码执行漏洞 (CVE-2023-26360)

1) 漏洞描述

Adobe ColdFusion 是一个商用的快速应用程序开发平台，ColdFusion 最初是为了创建能与数据库连接的网站而开发的。2.0 版本以后，它成为了一个全面的开发平台，包括一个集成开发环境以及功能全面的脚本语言。

ColdFusion 2018 在 Update 15 及之前版本/ColdFusion 2021 在 Update 5 及之前版本中存在远程代码执行漏洞，系统对用户输入的内容没有进行正确有效的校验，导致未授权的攻击者可以通过该利用获取服务器敏感信息。

2) 爆发时间

2023 年 3 月 15 日

3) 影响版本

ColdFusion 2018 <= Update 15

ColdFusion 2021 <= Update 5

4) 检测规则

检测流量中是否存在以下路径：

/cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/iedit.cfc?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://helpx.adobe.com/security/products/coldfusion/apsb23-25.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、仅允许可信 ip 访问 2、防止暴露在公网上

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/16363973847391969 28?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkFkb2JlJTIwQ29sZEZ1c2lvbiUyMCVFOCVCRiU5QyVFNyVBOCU4QiVFNCVCQiVBMyVFNyVBMCU4MSVFNiU4OSVBNyVFOCVBMSU4QyVFNiVCQyU4RiVFNiVCNCU5RShDVkUtMjAyMy0yNjM2MCklMjIlN0Q=&origin=intellList

3.4 瑞友天翼应用虚拟化系统 远程代码执行漏洞

1) 漏洞描述

瑞友天翼应用虚拟化系统是一种基于服务器计算架构的应用虚拟化平台，可以将各种应用软件集中部署在服务器上，客户端通过 WEB 访问授权的应用软件，实现远程接入和协同办公。

瑞友天翼应用虚拟化系统在 5.x 至 7.0.2.1 版本中存在远程代码执行漏洞。未授权的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) 爆发时间

2023 年 4 月 10 日

3) 影响版本

5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1

4) 检测规则

检测流量中是否存在以下路径：

/AgentBoard.XGI?user=

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：http://www.realor.cn/product/xiazaishiyong/

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/AgentBoard.XGI?user 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/1645359538255302656?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5MSU5RSVFNSU4RiU4QiVFNSVBNCVBOSVFNyVCRiVCQyVFNSVCQSU5NCVFNyU5NCVBOCVFOCU5OSU5QSVFNiU4QiU5RiVFNSU4QyU5NiVFNyVCMyVCQiVFNyVCQiU5RiUyMCVFOCVCRiU5QyVFOCVCMSU4MyVFNiU4OSVBNyVFNyVBOCU4QiVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.5 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) 爆发时间

2023 年 4 月 7 日

3) 影响版本

8.10.0 <= Apache Solr < 9.2.0

4) 检测规则

检测流量中是否存在以下路径：

/solr/admin/configs?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

请使用此产品的用户尽快打补丁或更新到最新版本：https://github.com/apache/solr/releases/tag/releases%2Fsolr%2F9.2.0

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. 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

VIP 平台链接：https://vip.tophant.com/detail/16477674056755486 72?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkFwYWNoZSUyMFNvbHIlMjAlRTglQkY1

OUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUoQ05WRC0yMDIzLTI3NTk4KSUyMiU3RA==&origin=intellList

3.6 Apache Druid 远程代码执行漏洞

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) 爆发时间

2023 年 4 月 19 日

3) 影响版本

Apache Druid <= 25.0.0

4) 检测规则

检测流量中是否存在以下路径：

/druid/indexer/v1/sampler?for=

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://druid.apache.org/docs/latest/development/extensions-core/druid-basic-security.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.防火墙规则： 使用防火墙规则限制对 Apache Druid 服务的访问，只允许

来自受信任网络的流量。

2.访问控制： 配置适当的访问控制，限制对 Apache Druid 的访问。只允许受信任的用户或 IP 地址访问服务。

VIP 平台链接：https://vip.tophant.com/detail/1648518584445571072?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkFwYWNoZSUyMERydWlkJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFJTIyJTdE&origin=intellList

3.7 PowerJob 未授权远程代码执行漏洞 (CVE-2023-29926)

1) 漏洞描述

PowerJob 是一个开源的分布式任务调度和计算框架，致力于提供简单易用、高可靠性、高伸缩性的任务执行和计算服务。

PowerJob V4.3.2 版本存在一个未授权接口，可以导致远程代码执行。

攻击者可以通过发送 HTTP 请求到 PowerJob 的/api/worker/execute 接口，携带恶意的 Java 代码片段，指定一个应用 ID 和一个任务 ID，从而触发远程代码执行，进而获取敏感信息，篡改数据，甚至控制整个系统

2) 爆发时间

2023 年 4 月 20 日

3) 影响版本

PowerJob V4.3.2

4) 检测规则

检测流量中是否存在以下路径：

/api/worker/execute

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://github.com/PowerJob/PowerJob/releases

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.访问控制： 配置适当的访问控制，限制对 PowerJob 服务的访问。只允许受信任的用户或 IP 地址访问服务。

2.网络隔离： 将 PowerJob 服务置于受控制的网络环境中，通过网络隔离减少潜在攻击者的访问机会。

3.防火墙规则： 使用防火墙规则限制对 PowerJob 服务的访问，只允许来自受信任网络的流量。

4.日志监控： 加强日志监控，定期审查 PowerJob 的访问日志和系统日志，以检测异常活动。

5.安全配置： 审查和强化 PowerJob 的安全配置选项，特别是与远程代码执行漏洞相关的设置，以最小化潜在的攻击面。

VIP 平台链接：https://vip.tophant.com/detail/1712307629533040640?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFOCU5MyU5RCVFNSU4NyU4Q09BJTIwZGF0YWpzb24lMjAlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlMjIlN0Q=&origin=intellList

3.8 DedeCMS 远程代码执行漏洞(CVE-2023-2928)

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 5.7.106 及之前版本存在代码注入漏洞。攻击者利用 uploads/dede/article_allowurl_edit.php 文件写入恶意 Webshell，在上传功能上传包含该文

件，从而进行远程代码执行。

2) 爆发时间

2023 年 5 月 27 日

3) 影响版本

DedeCMS <= 5.7.106

4) 检测规则

检测流量中是否存在以下路径：

dede/article_allowurl_edit.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

请用户尽快升级至最新版本，下载地址如下：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：限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2：文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

VIP 平台链接：https://vip.tophant.com/detail/1662428538856411136?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkRlZGVDTVMlMjAlRTglQkYlOUMlRTclQTglOEIlRTQlQkIlQTMlRTclQTAlODElRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUoQ1ZFLTIwMjMtMjkyOCklMjIlN0Q=&origin=intellList

3.9 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

检测流量中是否存在以下路径：

/admin/user_save.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：限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2：文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。

可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

VIP 平台链接：https://vip.tophant.com/detail/1663104023265415168?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNSVBNCVBNyVFNSU4RCU4RSVFNiU5OSVCQSVFNiU4NSVBNyVFNSU5QiVBRCVFNSU4QyVCQSVFNyVCQiVCQyVFNSU5MCU4OCVFNyVBRSVBMSVFNyU5MCU4NiVFNSVCOSVCMyVFNSU4RiVCMCUyMCVFOCVCRiU5QyVFNyVBOCU4QiVFNCVCQiVBMyVFNyVBMCU4MSVFNiU4OSVFNiVCNCU4RiVFNiVBMSU4QyVFNiVCNCU4RiVFNiVCNCU4RiU5RSUyMiU3RA==&origin=intellList

3.10 SugarCRM 远程代码执行漏洞(CVE-2023-22952)

1) 漏洞描述

SugarCRM 开源版是一款完全开放源代码的商业开源软件，具有界面活泼、简单易学的特点。美国 SugarCRM 公司是一间创立于 2006 年、但迅速在全球范围取得一定影响的客户关系管理软件厂商。

SugarCRM 在 12.0.2 之前和 11.0.5 之前的版本中存在一个远程代码执行漏洞，使用巧尽心思构建的请求，可以通过 EmailTemplates 注入自定义 PHP 代码，因为缺少输入验证。任何用户权限都可以利用此漏洞。

2) 爆发时间

2023 年 1 月 11 日

3) 影响版本

SugarCRM < 12.0.2

SugarCRM < 11.0.5

4) 检测规则

检测流量中是否存在以下路径：

/index.php

同时检测请求包中是否包含如下参数

module=Users&action=Authenticate&user_name=xxxxx &user_password=xxx
x

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://support.sugarcrm.com/Resources/Security/sugarcrm-sa-2023-001/

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。

2、配置防护设备以限制不可信 IP 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。

3、使用网络监控工具实时监控受影响的 SugarCRM 的网络流量和活动。这有助于及时发现潜在的攻击行为，并采取相应的应对措施。

VIP 平台链接：https://vip.tophant.com/detail/16131138867671900 16?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMlN1Z2FyQ1JNJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJThDJUU2JUJDJThGJUU2JUI0JTlFKENWRS0yMDIzLTIyOTUyKSUyMiU3RA==&origin=intellList

3.11 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) 爆发时间

2023 年 1 月 8 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

检测流量中是否存在 weblogic T3 序列化数据
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://support.oracle.com/rs?type=doc&id=2917213.2

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、针对 T3 协议使用连接筛选器临时阻止外部访问 7001 端口的 T3/T3s 协议：

连接筛选器：weblogic.security.net.ConnectionFilterImpl

2、在 Weblogic 控制台中，选择“base_domain”-<“监视”进入“AdminServer”-< “协议”-<“IIOP”中，取消“启用 IIOP”的勾选。并重启 Weblogic

项目，使配置生效。

VIP 平台链接：https://vip.tophant.com/detail/1615529624597565440?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMldlYmxvZ2ljJTIwJUU4JUJGJTlDJUU3JUE4JThCJUU0JUJCJUEzJUU3JUEwJTgxJUU2JTg5JUE3JUU4JUExJUE0JThDJUU2JUJDJThGJUU2JUI0JTlFKENWRS0yMDIzLTIxODM5KSUyMiU3RA==&origin=intellList

3.12 禅道项目管理系统 命令注入漏洞 (CNVD-2023-02709)

1) 漏洞描述

禅道研发项目管理软件存在命令注入漏洞。

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。

2) 爆发时间

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

检测流量中是否存在以下路径：

/misc-captcha-user.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

请用户尽快升级至最新版本，下载地址如下：https://www.zentao.net/禅道研发项目管理软件 > 18.0.beta1 (开源版)

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

VIP 平台链接：https://vip.tophant.com/detail/1611328448352096256?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyVBNiU4NSVFOSU4MSU5MyVFOSVBMSVCOSVFNyU5QiVBRSVFNyVBRSVBMSVFNyU5MCU4NiVFNyVCMyVCQiVFNyVCQiU5RiUyMCVFNSU5MSVCRCVFNCVCQiVBNCVFNiVCMyVBOCVFNSU4NSVBNSVFNiVCQyU4RiVFNiVCNCU5RShDTlZELTIwMjMtMDI3MDkpJTIyJTdE&origin=intellList

3.13TP-Link Archer AX21 AX1800 命令注入漏洞（CVE-2023-1389）

6) 漏洞描述

TP-LINK Archer AX21 是中国普联（TP-LINK）公司的一款无线路由器。

TP-LINK Archer AX21 1.1.4 Build 20230219 之前版本的 Web 管理界面的/cgi-bin/luci;stok=/locale 端点存在命令注入漏洞，该漏洞源于程序未对写入操作进行正确过滤，未经身份认证的攻击者可利用该漏洞以根权限注入并运行任意命令。

7) 爆发时间

2023 年 3 月 15 日

8) 影响版本

TP-LINK TP-Link Archer AX21 < 1.1.4 Build 20230219

9) 检测规则

检测流量中是否存在以下路径：

/cgi-bin/luci/;stok=/locale?form=

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

https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/ TP-Link Archer AX21 AX1800

VIP 平台链接：https://vip.tophant.com/detail/1636155463634653184?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMlRQLUxpbmslMjBBcmNoZXIlMjBBWDIxJTIwQVgxODAwJUU1JTkxJUJEJUU0JUJCJUE0JUU2JUIzJUE4JUU1JTg1JUE1JUU2JUJDJThGJUU2JUI0JTlFJTIwJUVGJUJDJTg4Q1ZFLTIwMjMtMTM4OSVFRiVCQyU4OSUyMiU3RA==&origin=intellList

3.14 VMware Aria Operations for Networks 命令注入漏洞(CVE-2023-20887)

11) 漏洞描述

VMware Aria Operations Networks 是一款网络和应用监控工具，可以帮助用户在多云环境中构建一个优化、高可用和安全的网络基础架构。

VMware Aria Operations Networks 在 6.x 版本中存在命令注入漏洞。这个漏洞将导致未授权的恶意攻击者在 VMware Aria Operations Networks 以 root 权限执行命令。

12) 爆发时间

2023 年 6 月 7 日

13) 影响版本

VMware Aria Operations Networks 6.x

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://www.vmware.com/security/advisories/VMSA-2023-0012.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. 首先，登录到受影响的 VMware Aria Operations Networks 系统。

2. 找到并备份受影响的配置文件。建议在进行任何修改之前，先备份原始文件：

cp /path/to/config_file /path/to/config_file.backup

3. 使用文本编辑器打开配置文件。例如，如果使用 vim 编辑器：

vim /path/to/config_file

4. 根据漏洞的具体情况和厂商建议，修改相关命令执行权限、环境变量或其他可能导致命令注入的设置。例如，禁用或添加限制条件，限制用户可执行的命令。

5. 保存修改并退出编辑器。

6. 重启相关服务或系统以使配置更改生效。例如：

systemctl restart aria_operations_service

7. 验证配置的修改是否生效，并测试系统功能以确保修改没有引入新的问题。

VIP 平台链接：https://vip.tophant.com/detail/1666475260859518976?keyword=

JTdCJTIya2V5d29yZCUyMiUzQSUyMlZNd2FyZSUyMEFyaWElMjBPcGVyYXRpb25zJTIwZm9yJTIwTmV0d29ya3MlMjAlRTUlOTElQkQlRTQlQkIlQTQlRTYlQjMlQTglRTUlODUlQTUlRTYlQkMlOEYlRTYlQjQlOUUoQ1ZFLTIwMjMtMjA4ODcpJTIyJTdE&origin=intellList

3.15 Apache Solr 命令执行漏洞(CNVD-2023-34111)

1) 漏洞描述

Apache Solr 是一个开源的搜索服务，使用 Java 语言开发，主要基于 HTTP 和 Apache Lucene 实现的。

Apache Solr 存在命令执行漏洞，攻击者可利用该漏洞在目标系统上执行任意代码。

2) 爆发时间

2023 年 5 月 6 日

3) 影响版本

Apache Solr <= 8.3.1

4) 检测规则

检测流量中是否存在以下路径：

/admin/info/system

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

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.关闭不必要的服务： 确保只开启系统中必需的服务，关闭不必要的服务，以减少攻击面。

2.更新到最新版本： 确保你的 Apache Solr 版本是最新的，因为漏洞可能已经在更新的版本中得到修复。及时应用厂商提供的安全更新是防范漏洞的有效方法。

3.访问控制： 配置适当的访问控制，限制对 Apache Solr 服务的访问。只允许受信任的 IP 地址访问 Solr 服务。

4.防火墙配置： 使用防火墙规则限制对 Solr 服务的访问，只允许来自信任网络的流量。

5.日志监控：加强日志监控，定期审查 Apache Solr 的访问日志和系统日志，以检测异常活动。

6.禁用不必要的功能： 如果可能，禁用不必要的功能和组件，以减少潜在的攻击面。

VIP 平台链接：https://vip.tophant.com/detail/16548591342915461l2?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMkFwYWNoZSUyMFNvbHIlMjAlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUoQ05WRC0yMDIzLTM0MTExKSUyMiU3RA==&origin=intellList

3.16 nginxWebUI 远程命令执行漏洞

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) 爆发时间

2023 年 6 月 28 日

3) 影响版本

nginxWebUI <= 3.4.6

4) 检测规则

检测流量中是否存在以下路径：

/AdminPage/conf/runCmd?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

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

VIP 平台链接：https://vip.tophant.com/detail/1673880200716357632?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMm5naW54V2ViVUklMjAlRTglQkYlOUMlRTclQTglOEIlRTUlOTElQkQlRTQlQkIlQTQlRTYlODklQTclRTglQTElOEMlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList

3.17 海康威视 iVMS-8700 综合安防管理平台软件 文件上传漏洞

6) 漏洞描述

海康威视 iVMS-8700 综合安防管理平台软件是一款集视频监控、报警管理、智能分析和门禁控制于一体的综合性安防管理软件。

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。

7) 爆发时间

2023 年 5 月 19 日

8) 影响版本

海康威视 iVMS-8700 综合安防管理平台软件

9) 检测规则

检测流量中是否存在以下路径：

/eps/api/resourceOperations/uploadsecretKeyIbuilding

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.hikvision.com/cn/support/Downloads/

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：限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2：文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

VIP 平台链接：https://vip.tophant.com/detail/1659446839474262016?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCNSVCNyVFNSVCQSVCNyVFNSVBOCU4MSVFOCVBNyU4NiUyMCUyMGlWTVMtODcwMCVFNyVCQiVCQyVFNSU5MCU4OCVFNSVBRSU4OSVFOSU5OCVCMiVFNyVBRSVBMSVFNyU5MCU4NiVFNSVCOSVCMyVFNSU4RiVCMCVFOCVCRCVBRiVFNCVCQiVCNiUyMCVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQyVBMCVFNiVCQyU4RiVFNiVCNCU5RSUyMiU3RA==&origin=intellList

3.18 泛微 e-cology9 协同办公系统 任意文件上传漏洞

11) 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 10.58.3 补丁之前存在任意文件上传漏洞。未经授权的攻击者可以上传恶意 Webshell 文件，从而控制服务器。

12) 爆发时间

2023 年 7 月 27 日

13) 影响版本

泛微 e-cology9 协同办公系统 < 10.58.3

14) 检测规则

检测流量中是否存在以下路径：

/E-mobile/App/Ajax/ajax.php?action=mobile_upload_save

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.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、限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2、文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。

可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件

3、强化访问控制：实施严格的访问控制措施，包括强密码策略、角色权限管理和多因素身份验证，以减少未授权访问和滥用漏洞的风险。

VIP 平台链接：https://vip.tophant.com/detail/1684402006783037440?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRWUtY29sb2d5OSVFNSU4RCU4RiVFNSU5MCU4QyVFNSU4QSU5RSVFNSU4NSVBQyVFNyVCMyVCQiVFNyVCQiU5RiUyMCVFNCVCQiVFNiU4NCU4RiVFNiU5NiU4NyVFNCVCNiVFNCVCOCU4QSVFNCVCQyU4MCU4RiVFNiU4RCU5RSUyMiU3RA==&origin=intellList

3.19 大华智慧园区综合管理平台 文件上传漏洞 (CVE-2023-3836)

16) 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。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。

17) 爆发时间

2023 年 7 月 22 日

18) 影响版本

大华智慧园区综合管理平台 <= 20230713 之前发行版本

19) 检测规则

检测流量中是否存在以下路径：

/emap/devicePoint_addImgIco?hasSubsystem=true

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。

20) 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.dahuatech.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、限制文件上传：通过限制用户上传文件的类型、大小和目标路径，可以有效减少任意文件上传漏洞的风险。例如，验证文件扩展名和内容，使用白名单机制，只允许特定的文件类型上传。

2、文件上传验证：在服务器接收到上传文件时，进行文件验证是很重要的。可以使用安全的文件验证机制，例如校验文件的魔术字节、文件头信息、文件结尾等，以确保上传的文件是预期的有效文件，并阻止上传恶意文件。

3、强化访问控制：实施严格的访问控制措施，包括强密码策略、角色权限管理和多因素身份验证，以减少未授权访问和滥用漏洞的风险

VIP 平台链接：https://vip.tophant.com/detail/1682843015179276288?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNSVBNCVBNyVFNSU4RCU4RSVFNiU5OSVCQSVFNiU4NSVBNyVFNSU5QiVBRCVFNSU4QyVCQSVFNyVCQiVCQyVFNSU5MCU4OCVFNyVBRSVBMSVFNyU5MCU4NiVFNSVCOSVCMyVFNSU4RiVCMCUyMCVFNiU5NiU4NyVFNCVCQiVCNiVFNCVCOCU4QSVFNCVCQSVCNCVFNiVCMCU5NSU5RShDVkUtMjAyMy0zODM2KSUyMiU3RA==&origin=intellList

3.20 泛微 e-cology9 协同办公系统 SQL 注入漏洞 (CNVD-2023-12632)

21) 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 10.56 版本之前存在 SQL 注入漏洞，攻击者无需身份认证即可获取数据库中敏感信息。

22) 爆发时间

2023 年 2 月 23 日

23) 影响版本

泛微 e-cology9 协同办公系统 < 10.56

24) 检测规则

检测流量中是否存在以下路径：

/mobile/plugin/browser.jsp

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。

25) 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/cs/securityDownload.asp

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/mobile/plugin 路由

VIP 平台链接：https://vip.tophant.com/detail/1628690780166164480?keyword=

JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNiVCMyU5QiVFNSVCRSVBRWUtY29sb2d5OSVFNSU4RCU4RiVFNSU5MCU4QyVFNSU4QSU5RSVFNSU4NSVBQyVFNyVCMyVCQiVFNyVCQiU5RiUyMFNRTCVFNiVCMyVBOCVFNSU4NSVBNSVFNiVCQyU4RiVFNiVCNCU5RShDTlZELTIwMjMtMTI2MzIpJTIyJTdE&origin=intellList

3.21 畅捷通 T+ SQL 注入漏洞

26) 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。

27) 爆发时间

2023 年 6 月 9 日

28) 影响版本

畅捷通 T+ 13.0

畅捷通 T+ 16.0

29) 检测规则

检测流量中是否存在以下路径：

/tplus/ajaxpro/Ufida.T.SM.UIP.MultiCompanyController,Ufida.T.SM.UIP.ashx?method=CheckMutex

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。

30) 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.chanjetvip.com/product/goods/

VIP 平台链接：https://vip.tophant.com/detail/1666980164946497536?keyword=JTdCJTIya2V5d29yZCUyMiUzQSUyMiVFNyU5NSU4NSVFNiU4RCVCNyVFOSU4MCU5QVQlMkIlMjBTUUwlRTYlQjMlQTglRTUlODUlQTUlRTYlQkMlOEYlRTYlQjQlOUUlMjIlN0Q=&origin=intellList