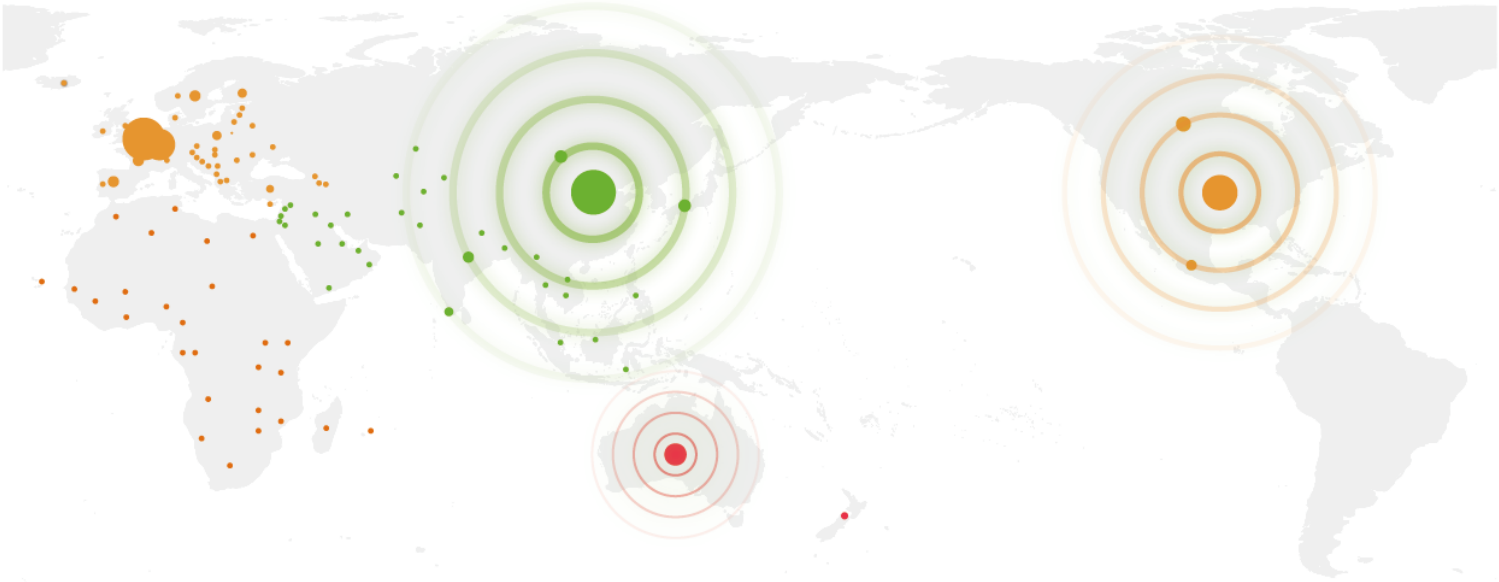
# 绿盟威胁情报周报

2023年第26周（2023.06.19-2023.06.25）



绿盟威胁情报中心（NTI）

https://nti.nsfocus.com/

# 本周热点概览

## 威胁通告

- VMware Aria Operations for Networks 远程代码执行漏洞（CVE-2023-20887）
- 微软 6 月安全更新多个产品高危漏洞通告
- Smartbi 商业智能软件绕过登录漏洞通告
- Openfire 控制台身份认证绕过漏洞（CVE-2023-32315）通告
- 用友畅捷通 T+ SQL 注入漏洞和反序列化漏洞通告

## 热点资讯

- 网络罪犯正在利用矿池洗钱
- 黑客使用假的 OnlyFans 图片来植入窃取信息的恶意软件
- VMware 已确认 CVE-2023-20887 已被在野利用
- DIICOT 网络犯罪团伙扩大攻击能力
- 对欧洲投资银行和 Redditt 的网络攻击
- 暗网上发现数百万英国大学证书
- DoNot 黑客组织在 Google Play 商店部署恶意 Android 应
- Rhysida 勒索软件盗取大量智利军方文件
- 深入 WASP 的巢穴：深入调查由 PYPI 托管的恶意软件
- 数百万俄勒冈州和路易斯安那州的身份证在 MOVEit 漏洞中

# 威胁通告

1.VMware Aria Operations for Networks 远程代码执行漏洞（CVE-2023-20887）

【标签】VMware

【发布时间】2023-06-19 10:00:00 GMT

【概述】

近日，绿盟科技 CERT 监测到 VMware Aria Operations for Networks 远程代码执行漏洞。由于 createSupportBundle 方法中存在特定缺陷，执行系统调用时未正确验证用户输入的字符串，未经身份验证的远程攻击者可通过命令注入的方式利用该漏洞，最终可实现在目标系统上以 root 权限执行任意代码。目前该漏洞细节及 PoC 已公开，请相关用户尽快采取措施进行防护。

【参考链接】

https://nti.nsfocus.com/threatNotice

2.微软 6 月安全更新多个产品高危漏洞通告

【标签】微软

【发布时间】2023-06-19 09:00:00 GMT

【概述】

6 月 14 日，绿盟科技 CERT 监测到微软发布 6 月安全更新补丁，修复了 77 个安全问题，涉及 Microsoft SharePoint Server、Windows Pragmatic General Multicast （PGM）、Microsoft Exchange Server、Microsoft Excel、.NET、.NET Framework 和 Visual Studio 等广泛使用的产品，其中包括权限提升、远程代码执行等高危漏洞类型。

【参考链接】

https://nti.nsfocus.com/threatNotice

3.Smartbi 商业智能软件绕过登录漏洞通告

【标签】Smartbi

【发布时间】2023-06-19 09:00:00 GMT

【概述】

近日，绿盟科技 CERT 监测到 Smartbi 官方修复了一个绕过登录漏洞，在某种特定情况下存在默认用户任意登录问题，未经身份验证的攻击者通过该漏洞可获取系统中敏感信息，最终造成敏感信息泄露。

【参考链接】

https://nti.nsfocus.com/threatNotice

4.Openfire 控制台身份认证绕过漏洞通告（CVE-2023-32315）

【标签】Openfire

【发布时间】2023-06-19 09:00:00 GMT

【概述】

近日，绿盟科技 CERT 监测到 Openfire 控制台身份认证绕过漏洞（CVE-2023-32315）。Openfire 的管理控制台（Admin Console）是一个基于 Web 的应用程序，它被发现容易受到通过设置环境进行的路径遍历攻击，未经身份验证的攻击者在已配置的 Openfire 环境中使用未经身份验证的 Openfire 设置环境来访问管理员用户界面，从而获取服务器权限，最终实现在目标系统上执行任意代码。目前该漏洞细节及 PoC 已公开。请相关用户尽快采取措施进行防护。

【参考链接】

https://nti.nsfocus.com/threatNotice

5.用友畅捷通 T+ SQL 注入漏洞和反序列化漏洞通）

【标签】不区分行业

【发布时间】2023-06-19 09:00:00 GMT

【概述】

近日，绿盟科技 CERT 监测到用友畅捷通 T+存在 SQL 注入漏洞和反序列化漏洞。目前漏洞的 PoC 已公开，请受影响的用户尽快采取措施进行防护。用友畅捷通 T+SQL 注入漏洞，未经身份认证的远程攻击者可在易受攻击系统上执行任意 SQL 语句，某些情况下攻击者利用该漏洞可在底层操作系统上执行 shell 命令。用友畅捷通 T+反序列化漏洞，未经身份认证的远程攻击者可构造特定请求上传恶意文件到目标系统，从而在服务器上执行任意代码。用友畅捷通 T+是一款基于互联网的新型企业管理软件，功能模块包括：财务管理、采购管理、库存管理等。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。

【参考链接】

https://nti.nsfocus.com/threatNotice

# 热点资讯

1.网络罪犯正在利用矿池洗钱

【标签】不区分行业

【概述】

据 chainanalysis 称，网络犯罪分子越来越多地将犯罪所得转移到加密矿池，以混淆其来源。这家区块链分析公司表示，矿池使矿工能够组合他们的计算资源，被这些恶意行为者用作事实上的混合器。

【参考链接】

https://ti.nsfocus.com/security-news/79vRoL

2.黑客使用假的 OnlyFans 图片来植入窃取信息的恶意软件

【标签】DcRAT

【概述】

恶意软件活动使用虚假的 OnlyFans 内容和成人诱饵来安装称为“DcRAT”的远程访问木马，允许威胁行为者窃取数据和凭据或在受感染的设备上部署勒索软件。OnlyFans 是一项内容订阅服务，付费订阅者可以访问成人模特、名人和社交媒体名人的私人照片、视频和帖子。它是一个广泛使用的网站和一个知名度很高的名称，因此它可以吸引那些希望免费访问付费内容的人们。eSentire 发现的新活动自 2023 年 1 月以来一直在进行，传播包含 VBScript 加载程序的 ZIP 文件，受害者被诱骗手动执行，以为他们将要访问高级 OnlyFans 内容。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpL

3.VMware 已确认 CVE-2023-20887 已被在野利用

【标签】VMware

【概述】

这家虚拟化技术巨头周二更新了一份关键级别的公告，向运行网络监控软件的企业发出直言不讳的警告：“VMware 已确认 CVE-2023-20887 的利用已在野外发生。”这些实时漏洞首先由 GreyNoise 标记，目标是 CVE-2023-20887 命令注入漏

洞，该漏洞的 CVSS 严重性评分为 9.8/10。VMware 在本月早些时候发布的一份公告中表示：“具有 VMware Aria Operations for Networks 网络访问权限的恶意行为者可能能够执行命令注入攻击，从而导致远程代码执行。”

【参考链接】

https://ti.nsfocus.com/security-news/79vRpR

4. DIICOT 网络犯罪团伙扩大攻击能力

【标签】DIICOT

【概述】

研究人员发现，有证据表明，Diicot 威胁行为者正在通过新的有效载荷和 Cayosin 僵尸网络扩展他们的能力。专家们发现了几个有效载荷，其中一些尚未公开，它们被用作正在进行的新活动的一部分。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpx

5.对欧洲投资银行和 Redditt 的网络攻击

【标签】银行

【概述】

根据最近的报道，欧洲投资银行(EIB)似乎成为了俄罗斯黑客组织 Killnet 精心策划的网络攻击的受害者。这些黑客从 5 月份就开始策划这次数字攻击，目标是在本月底前瘫痪西方金融体系。据推测，这次袭击可能是为了报复包括英国和美国在内的几个国家在乌克兰与克里姆林宫的冲突中向乌克兰提供的援助。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpH

6.暗网上发现数百万英国大学证书

【标签】不区分行业

【概述】

安全研究人员在暗网上发现了 220 万份与英国 100 所顶尖大学相关的泄露证书，使教职员工、学生及其数据处于危险之中。Crossword Cybersecurity 的万亿风险监控服务发现了这些凭证，其中超过一半(54%)属于罗素集团(russell Group)的精英机构。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpn

7. DoNot 黑客组织在 Google Play 商店部署恶意 Android 应用程序

【标签】DoNot

【概述】

国家支持的威胁行为者使用 Google Play 上的三个 Android 应用程序从目标设备收集情报，例如位置数据和联系人列表。这些恶意 Android 应用程序是由 Cyfirma 发现的 ，他以中等可信度将此操作归因于印度黑客组织“DoNot”，该组织也被追踪为 APT-C-35，该组织至少从 2018 年开始就以东南亚的知名组织为目标。Cyfirma 在 Google Play 上发现的可疑应用程序是 nSure Chat 和 iKHfaa VPN，它们都是从“SecurITY Industry”上传的。根据 Cyfirma 的说法，这两款应用程序和来自同一发行商的第三款应用程序似乎没有恶意，但仍可在 Google Play 上使用。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpF

8.Rhysida 勒索软件盗取大量智利军方文件

【标签】Rhysida

【概述】

Bleeping Computer 网站披露，一个名为 Rhysida 的勒索软件团伙在网上泄露了声称从智利军队（Ejército de Chile）网络中窃取的文件。网络攻击者入侵系统后，智利方面立刻启动了网络隔离，军事安全专家开始对受影响系统的进行修复，并向智利参谋长联席会议计算机安全事件响应小组（CSIRT）和国防部报告了这一事件。巧合的是，网络攻击事件披露几天后，当地媒体报道称一名陆军下士因参与勒索软件攻击被捕。

【参考链接】

https://ti.nsfocus.com/security-news/79vRpf

9.深入 WASP 的巢穴：深入调查由 PYPI 托管的恶意软件

【标签】PYPI

【概述】

在 2022 年底，我们决定开始监控 PyPI，可以说是最重要的 Python 存储库，因为有许多关于它托管恶意软件的报告。在这篇文章中，我们将分享对 PyPi 可疑库的见解，并仔细研究滥用它的特定活动。

【参考链接】

https://ti.nsfocus.com/security-news/79vRp9

10.数百万俄勒冈州和路易斯安那州的身份证在 MOVEit 漏洞中被盗

【标签】MOVEit

【概述】

路易斯安那州和俄勒冈州警告称，一个勒索软件团伙入侵了他们的 MOVEit Transfer 安全文件传输系统，窃取了存储的数据，数百万份驾驶执照在数据泄露中暴露出来。这些攻击是由 Clop 勒索软件操作进行的，该操作于 5 月 27 日开始在全球范围内攻击 MOVEit Transfer 服务器，使用了一个以前未知的零日漏洞 CVE-2023-34362。这些攻击导致了全球范围内数据泄露的广泛披露，影响了公司、联邦政府机构和地方州政府机构。

【参考链接】

https://ti.nsfocus.com/security-news/79vRoP

## 绿盟威胁情报中心

绿盟威胁情报中心（NSFOCUS Threat Intelligence），作为绿盟科技智慧安全 3.0 战略的重要组成部分，统筹公司的威胁情报生态和能力建设，对外提供威胁情报产品和服务。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

绿盟威胁情报中心：https://nti.nsfocus.com/

绿盟威胁情报云：https://ti.nsfocus.com/


总部：北京市海淀区北洼路 4 号益泰大厦
绿盟科技（股票代码 300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：NTI@nsfocus.com