深信服智安全
SANGFOR SECURITY

5 月份安全威胁通告（上）

(20240501 期)

深信服科技股份有限公司

2024 年 5 月 20 日

■ 信息来源

国家信息安全漏洞共享平台（CNVD）

国家互联网应急响应中心（CNCERT/CC）

深信服千里目安全技术中心

深信服云端威胁对抗指挥中心

深信服安全 BG - 全球安全运营中心

■ 编辑/审阅

深信服千里目安全技术中心

深信服安全 BG - 全球安全运营中心

说明

本通告涵盖 2024 年 5 月份（5.1-5.15）深信服团队发现的新增安全漏洞，并将此月份国际国内发生的热点安全事件进行总结整理，以期达到及时分享网络安全现状及最新网络安全热点事件的目的，欢迎业内人士讨论指正。文档内引用了部分互联网已公开的数据信息，已在文档里标明出处。

本期可以关注 Apache ActiveMQ API 未授权访问漏洞、Apache Kafka 访问控制漏洞、Util-linux wall 权限提升漏洞和瑞友天翼应用虚拟化系统远程代码执行漏洞，CNVD 和微软发布了安全通告及漏洞详情，建议受影响用户及时更新升级至最新版本。

本期网络安全政策法律动态信息：

中央网信办等四部门印发《2024 年数字乡村发展工作要点》

关于 16 项网络安全国家标准获批发布的通知

深信服安全团队拥有优秀的安全技术专家，可扫码关注深信服千里目安全技术中心微信公众号，第一时间了解最新的安全事件、威胁漏洞情报等。

深信服千里目安全技术中心公众号二维码

目 录

一、 安全风险通告 1
（一）Apache ActiveMQ API 未授权访问漏洞 1
（二）Apache Kafka 访问控制漏洞 3
（三）Util-linux wall 权限提升漏洞 5
（四）瑞友天翼应用虚拟化系统远程代码执行漏洞 6
二、 安全事件分析 8
（一） 【高级威胁追踪(APT)】警惕来自 Timitator 组织 RUST 特马的攻击 8
三、安全热点 21
（一）伦敦证券旗下数据库被窃取，泄露超 500 万条敏感信息 21
（二）超 5 万台 Tinyproxy 服务器易受严重 RCE 漏洞影响 23
（三）英国防部超 22.5 万名军事人员信息遭泄露 24
四、网络安全政策法律动态 25
（一）中央网信办等四部门印发《2024 年数字乡村发展工作要点》 25
（二）关于 16 项网络安全国家标准获批发布的通知 26
五、微软安全通告 26
（一） 漏洞概要 26
（二） 漏洞数据分析 27
1 漏洞数量趋势 27
2 历史微软补丁日 5 月漏洞对比 27
3 漏洞数量分析 29
（三） 重要漏洞分析 30
1 漏洞分析 30
2 影响范围 31
3 修复建议 34
六、CNVD 漏洞收录情况 35
（一） 漏洞分类统计 35
（二） 漏洞关注情况 36
（三） 漏洞趋势 37
附录：4 月份重要漏洞信息汇总 39

一、安全风险通告

Apache ActiveMQ API 未授权访问漏洞

漏洞名称：Apache ActiveMQ API 未授权访问漏洞

漏洞描述：2024 年 5 月 8 日，深瞳漏洞实验室监测到一则 Apache ActiveMQ 组件存在未授权访问漏洞的信息，由于 ActiveMQ 未对 Jolokia JMX REST API 和 Message REST API 添加身份校验，未授权的攻击者可利用暴露通过 Jolokia JMX REST API 与消息代理进行交互，或者使用 Message REST API 发送和接收消息，**最终导致敏感信息泄露和数据受损**。

漏洞编号：CVE-2024-32114，漏洞威胁等级：**高危**。

组件介绍：

Apache ActiveMQ 是最流行的开源、多协议、基于 Java 的消息代理。它支持行业标准协议，因此用户可以从多种语言和平台的客户端选择中受益。从使用 JavaScript、C、C++、Python、.Net 等编写的客户端进行连接。

影响范围：

目前受影响的 Apache ActiveMQ 版本：

6.0.0 ≤ Apache ActiveMQ < 6.1.2

利用条件：

1、用户认证：否

2、前置条件：默认配置

3、触发方式：远程

<综合评定利用难度>：未知。

<综合评定威胁等级>：高危，能造成敏感信息泄露和数据受损。

官方解决方案：

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://issues.apache.org/jira/browse/AMQ-9477

深信服解决方案：

1.风险资产发现

支持对 Apache ActiveMQ 的**主动检测**，可**批量检出**业务场景中该事件的**受影响资产**情况，相关产品如下：

【深信服主机安全检测响应平台 CWPP】已发布资产检测方案。

【深信服云镜 YJ】已发布资产检测方案。

【深信服漏洞评估工具 TSS】已发布资产检测方案。

2.漏洞主动扫描

支持对 Apache ActiveMQ API 未授权访问漏洞的**主动扫描**，可**批量快速**检出业务场景中是否存在漏洞风险，相关产品如下：

【深信服漏洞评估工具 TSS】预计 2024 年 5 月 9 日发布扫描方案。

【深信服安全托管服务 MSS】预计 2024 年 5 月 9 日发布扫描方案。（需要具备 TSS 组件能力）

Apache Kafka 访问控制漏洞

漏洞名称：Apache Kafka 访问控制漏洞

漏洞描述：2024 年 5 月 8 日，深瞳漏洞实验室监测到一则 Apache-Kafka 组件存在访问控制错误漏洞的信息，Apache Kafka 中存在一个访问控制漏洞，当 Apache Kafka 集群从 ZooKeeper 模式迁移到 KRaft 模式时，如果管理员删除 ACL（访问控制列表），并且与删除的 ACL 相关联的资源在删除后仍有两个以上其他 ACL 关联时，将导致 ACL 可能无法正确执行，**该漏洞可能导致未授权访问和拒绝服务攻击。**

漏洞编号：CVE-2024-27309，漏洞威胁等级：**高危**。

组件介绍：

Apache Kafka 是一个开源分布式事件流平台，被数千家公司用于高性能数据管道、流分析、数据集成和任务关键型应用程序。

影响范围：

目前受影响的 Apache Kafka 版本：

3.5.0 ≤ Kafka ≤ 3.5.2

3.6.0 ≤ Kafka ≤ 3.6.1

利用条件：

1、用户认证：需要管理员权限

2、前置条件：集群从 ZooKeeper 模式迁移到 KRaft 模式

3、触发方式：远程

<综合评定利用难度>：未知。

<综合评定威胁等级>：高危，能造成拒绝服务。

官方解决方案：

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://lists.apache.org/thread/6536rmzyg076lzzdw2xdktvnz163mjpy

深信服解决方案

1.风险资产发现

支持对 Apache Kafka 的**主动检测**，**可批量检出**业务场景中该事件的**受影响资产**情况，相关产品如下：

【深信服主机安全检测响应平台 CWPP】已发布资产检测方案。

【深信服云镜 YJ】已发布资产检测方案。

【深信服漏洞评估工具 TSS】已发布资产检测方案。

2.漏洞主动扫描

支持对 Apache Kafka 访问控制漏洞的主动扫描，可批量快速检出业务场景中是否存在漏洞风险，相关产品如下：

【深信服漏洞评估工具 TSS】预计 2024 年 5 月 9 日发布扫描方案。

【深信服安全托管服务 MSS】预计 2024 年 5 月 9 日发布扫描方案。（需要具备 TSS 组件能力）

Util-linux wall 权限提升漏洞

漏洞名称：Util-linux wall 权限提升漏洞

漏洞描述：2024 年 5 月 8 日，深瞳漏洞实验室监测到一则 util-linux 组件存在信任管理问题漏洞的信息，util-linux 2.40 版本中的 wall 命令存在设计缺陷，由于 util-linux 允许通过 argv 将转义序列发送到其他用户的终端。**攻击者利用该漏洞可控制其他账户并提升权限。**

漏洞编号：CVE-2024-28085，漏洞威胁等级：**高危**。

组件介绍：

util-linux 是 Linux 内核使用的标准包，包含了许多基本的系统工具，能够执行各种任务，如文件和磁盘管理、性能监控等，是进行系统维护和管理的基础。

影响范围：

目前受影响的 Linux 版本：

Util-linux < 2.40

官方解决方案：

当前官方已发布受影响版本的对应补丁，建议受影响的用户及时更新官方的安全补丁。

链接如下：

https://mirrors.edge.kernel.org/pub/linux/utils/util-linux/v2.40/

瑞友天翼应用虚拟化系统远程代码执行漏洞

漏洞名称：瑞友天翼应用虚拟化系统远程代码执行漏洞

漏洞描述：2024 年 5 月 10 日，深瞳漏洞实验室监测到一则瑞友天翼应用虚拟化系统组件存在代码注入漏洞的信息，瑞友天翼应用虚拟化系统存在远程代码执行漏洞，攻击者可以在未授权的状态下利用该漏洞上传任意文件，执行恶意代码，导致服务器失陷。

漏洞威胁等级：**高危**。

组件介绍：

瑞友天翼应用虚拟化系统是国内具有自主知识产权的应用虚拟化平台，是基于服务器计算的应用虚拟化平台。它将用户所有应用软件集中部署在天翼服务器上，客户端通过 Web 即可快速安全地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，从而为用户打造集中、便捷、安全、高效的虚拟化支撑平台。

影响范围：

目前受影响的瑞友天翼应用虚拟化系统版本：

瑞友天翼应用虚拟化系统 ≤ 7.0.5.1

利用条件：

1、用户认证：无需用户认证

2、前置条件：默认配置

3、触发方式：远程

<综合评定利用难度>：容易，无需授权即可远程代码执行。

<综合评定威胁等级>：高危，能造成远程代码执行。

官方解决方案：

官方已发布最新补丁修复该漏洞，补丁号：GWT7.0.5_patch_202405081139。请联系官方获取补丁包修复。

深信服解决方案：

1.风险资产发现

支持对瑞友天翼应用虚拟化系统的**主动检测**，**可批量检出**业务场景中该事件的受影响资产情况，相关产品如下：

【深信服主机安全检测响应平台 CWPP】已发布资产检测方案。

【深信服云镜 YJ】已发布资产检测方案。

2.漏洞主动检测

支持对瑞友天翼应用虚拟化系统远程代码执行漏洞的主动检测，可批量快速检出业务场景中是否存在漏洞风险，相关产品如下：

【深信服云镜 YJ】预计 2024 年 5 月 15 日发布检测方案。

【深信服漏洞评估工具 TSS】预计 2024 年 5 月 23 日发布检测方案。

【深信服安全托管服务 MSS】预计 2024 年 5 月 23 日发布检测方案（需要具备 TSS 或 CWPP 组件能力）。

【深信服安全检测与响应平台 XDR】预计 2024 年 5 月 15 日发布检测方案（需要具备云镜或 CWPP 组件能力）。

二、安全事件分析

（一） 【高级威胁追踪(APT)】警惕来自 Timitator 组织 RUST 特马的攻击

1 概述

Timitator(战术模仿者) 组织自 2022 年到 2023 年针对我国的能源、高校、科研机构及军工等行业进行攻击，主要采取鱼叉、nday 等方式进行打点。

其鱼叉攻击分别投递过 exe、chm、iso(img)及 lnk 等格式的载荷，在受害者成功执行该恶意附件后，在第一阶段时其会加载 cobaltstrike 并建立稳定连接，在第二阶段通过 cobaltstrike 加载其自定义特马，再通过探测内网确认每个失陷目标的价值，对不同的目标设计不同的后续攻击或利用方式，窃取高价值目标的数据和文件。该组织在攻击行动中常模仿其他组织的攻击战术，因此我们将该组织命名为战术模仿者(Timitator->ttps imitator)，该组织也被其他友商称为 apt-q-77、变异鼠，部分友商将其归因到海莲花，该组织目前归因复杂无法确定其最终背景 。

近期，深信服深瞻情报实验室捕获到 Timitator 组织最新的一批钓鱼样本，在这批样本中发现该组织在攻击中使用 RUST 特马代替 CobaltStrike 进行远程控制，并且发现释放到磁盘中的文件带有 VMP 虚拟外壳。

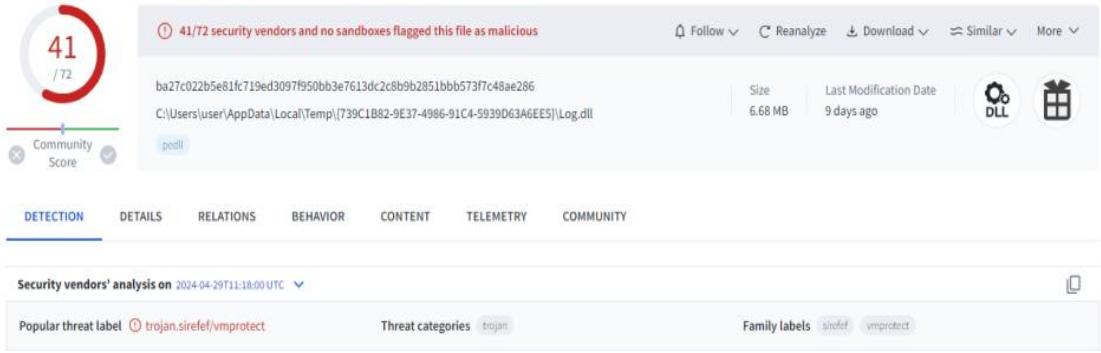
本次捕获到多个 Timitator 钓鱼样本，分析后发现：在 2024-03-28 之后上传的样本中，没有使用 CobaltStrike 作为远控工具，而是使用一个由 RUST 语言编写的远控工具，在文章中简称为 RUST 特马。

sha256	上传时间	type	C2
49d3777d0d02cd2a4d1c44313c72279fee1681c1e3566535f9117d17b274424b	2024-03-22	CobaltStrike	39.104.205.68:443
acf0fb4dac33e197de3a3e142eeaa7e5a892607424e8ea8708d49c65f3703d61	2024-03-25	CobaltStrike	64.176.58.16:80
87bfce678855fa498d85b143beaf129f9bd468ebdcc1226b2ba39780a02f3d2e	2024-03-28	RUST 特马	38.180.94.8:80
aac2cbd4cb119dec6c9a8c58f86b8bdd83d27fdaed85149bb2572599de9e32c0	2024-04-12	RUST 特马	38.180.94.8:80

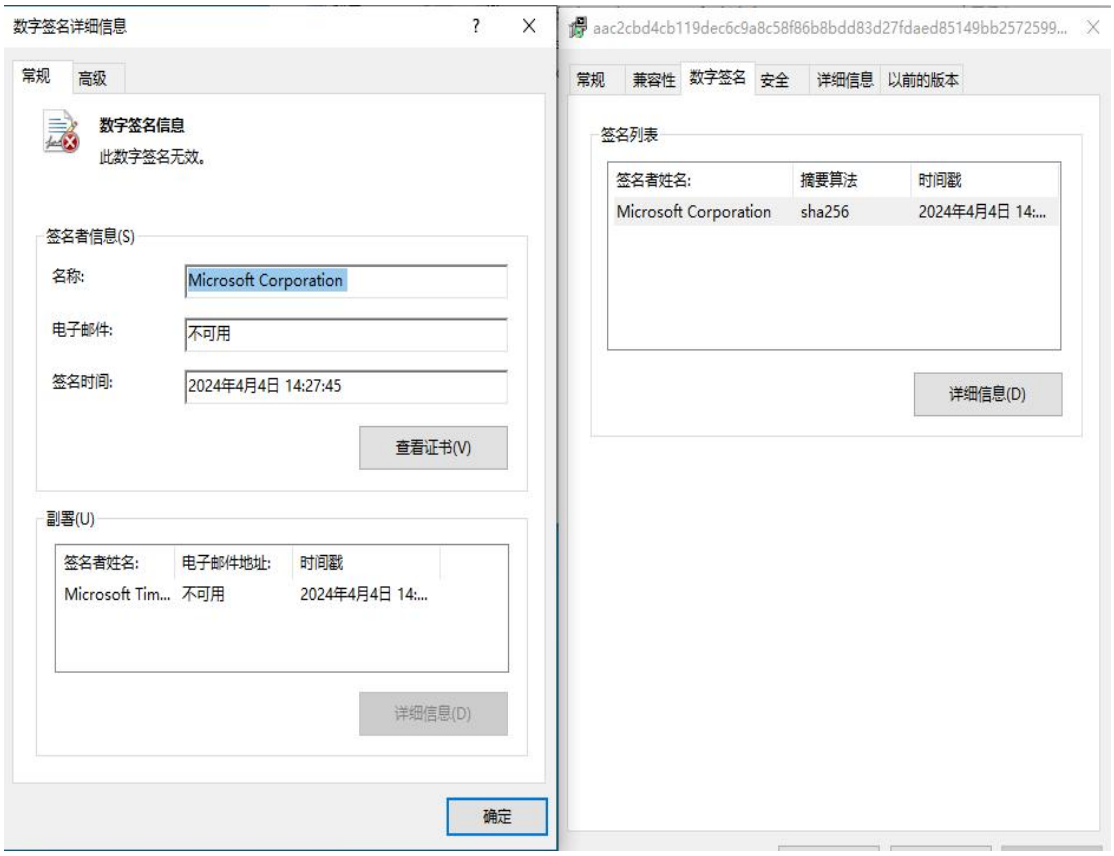
该组织曾多次使用白加黑技术，此次样本中使用两种白加黑利用组合。

Psadminagent.exe(nitrosense 散热控制系统)+WTSAPI32.dll
Bitdefender(杀毒软件)+Log.dll

释放到磁盘中的恶意 dll 文件，则是意外地使用 VMP 加壳来保护程序，但因为没有合法的签名，导致免杀效果不佳。



本次制作成钓鱼样本的 EXE 文件，为 NSIS 打包而成安装程序，最新的样本中还发现带有伪造的 Microsoft 签名以及伪造成某国内企业的描述信息，用于伪装成正常的软件程序。



2 样本分析

以其中一个 NSIS 打包的安装程序为例，该样本的详细信息如下

描述	详细信息
名称	1.exe
文件大小	17185768 bytes
文件类型	EXE
文件功能	Loader
编译时间	/
开发平台及语言	/
是否加壳	否
VT 首次上传时间	2024-04-12 07:56:11 UTC
md5	4a2e2fe59c21cbefbbad3bb8d2852a44
Sha256	aac2cbd4cb119dec6c9a8c58f86b8bdd83d27fdaed85149bb2572599de9e32c0

文件执行后会在%temp%目录释放文件夹{739C1B82-9E37-4986-91C4-5939D63A6EE5}和 3 个可执行文件，然后执行 setup.exe，从而加载恶意程序 Log.dll。

第二阶段载荷的详细信息如下。

描述	详细信息
名称	Log.dll
文件大小	7006208 bytes
文件类型	DLL
文件功能	Loader
编译时间	/
开发平台及语言	/
是否加壳	VMProtect
VT 首次上传时间	2024-03-28 05:06:56 UTC
md5	aff6cae1b461c830f6cf0efe2364101d
Sha256	ba27c022b5e81fc719ed3097f950bb3e7613dc2c8b9b2851bbb573f7c48ae286

该文件原始文件名为 snvmse.dll，功能与以往发现的样本一致，执行后会生成文件夹%temp%\NVidiaSetup\kd8812u，将计算机名和 C 盘信息写入到 kd8812u 的附加数据流。

随后使用 loadlibrary 加载另一个恶意程序 SogouInput.dll，调用其导出函数 begin。

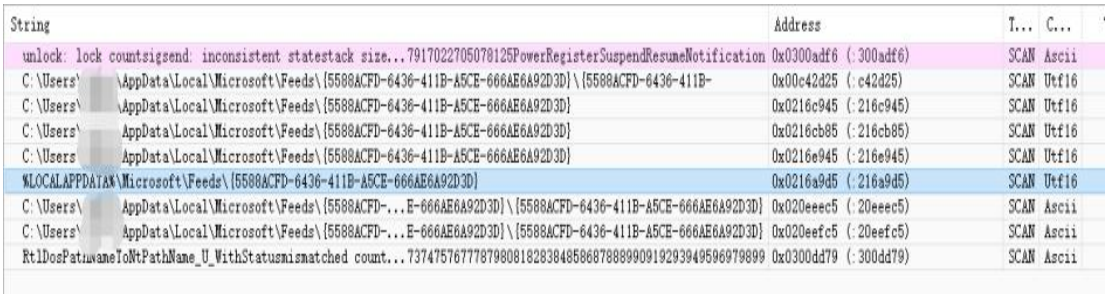
String	Address	T...	C...	Tag	C...	S...	X...
\Device\HarddiskVolume3\Users\ \AppData\Local\Temp\{739C1B82-9E37-4986-91C4-5939D63A6EE5}\SogouInput.dll	0x00274cd9 (:274cd9)	SCAN	Utf16	PATH	108	133	0
C:\Users\ \AppData\Local\Temp\{739C1B82-9E37-4986-91C4-5939D63A6EE5}\SogouInput.dll	0x00003aec (:3aec)	SCAN	Utf16	PATH	87	131	0
C:\Users\ \AppData\Local\Temp\{739C1B82-9E37-4986-91C4-5939D63A6EE5}\SogouInput.dll	0x002cc095 (:2cc095)	SCAN	Utf16	PATH	87	131	0
SogouInput.dll	0x00c37495 (:c37495)	SCAN	Utf16	DLL	14	92	0
SogouInput.dll	0x0413f2d5 (:413f2d5)	SCAN	Utf16	DLL	14	92	0

SogouInput.dll 文件信息如下。

描述	详细信息
名称	SogouInput.dll
文件大小	10268160 bytes
文件类型	DLL
文件功能	Loader
编译时间	/
开发平台及语言	/
是否加壳	否
VT 首次上传时间	2024-03-28 05:06:58 UTC
md5	9476ae68b01c0167254b3ec638e619b9
Sha256	6cb80b939b8de9f15726391f807b947951083da28c2647b8c8451021d559f7ee

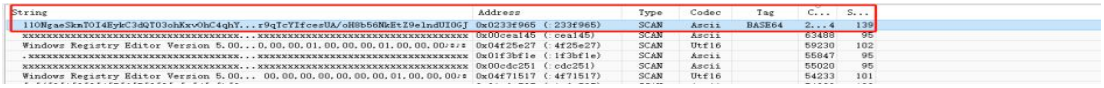
该组件也沿用以往的设计，截取屏幕截图保存为 0_1718x926.png，收集系统信息保存为{5588ACFD-6436-411B-A5CE-666AE6A92D3D}。

String	Address	T...	C...	Tag	C..
C:\Users\ \AppData\Roaming\Identities\{83AF1370-986F-1673-091A-02681FA62C3B}\0_1718x926.png	0x0218c945 (:218c945)	SCAN	Utf16	PATH	9
C:\Users\ \AppData\Roaming\Identities\{83AF1370-986F-1673-091A-02681FA62C3B}\0_1718x926.png	0x02108a65 (:2108a65)	SCAN	Ascii	PATH	9
C:\Users\ \AppData\Roaming\Identities\{83AF1370-986F-1673-091A-02681FA62C3B}\0_1718x926.png	0x02108ac5 (:2108ac5)	SCAN	Ascii	PATH	9
= flushGen gfreecnt= pages at runqsize= runqueue= s...stVirtualUnlockVTSFreeMemoryWriteConsoleWadvapi32.dll	0x03003c7b (:3003c7b)	SCAN	Ascii	PATH	501



String	Address	T...	C...
unlock: lock countsigsend: inconsistent statestack size...7917022705078125PowerRegisterSuspendResumeNotification	0x0300adf6 (:300adf6)	SCAN	Ascii
C:\Users\ \AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}\{5588ACFD-6436-411B-	0x00c42d25 (:c42d25)	SCAN	Utf16
C:\Users\ \AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x0216c945 (:216c945)	SCAN	Utf16
C:\Users\ AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x0216cb85 (:216cb85)	SCAN	Utf16
C:\Users\ AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x0216e945 (:216e945)	SCAN	Utf16
%LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x0216a9d5 (:216a9d5)	SCAN	Utf16
C:\Users\ AppData\Local\Microsoft\Feeds\{5588ACFD-...E-666AE6A92D3D}\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x020eeec5 (:20eeec5)	SCAN	Ascii
C:\Users\ AppData\Local\Microsoft\Feeds\{5588ACFD-...E-666AE6A92D3D}\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}	0x020eefc5 (:20eefc5)	SCAN	Ascii
RtlDosPathNameToNtPathName_U_WithStatusmismatched count...73747576777879808182838485868788899091929394959679899	0x0300dd79 (:300dd79)	SCAN	Ascii

随后在导出函数 begin 中从资源中读取出 shellcode，解密后执行。

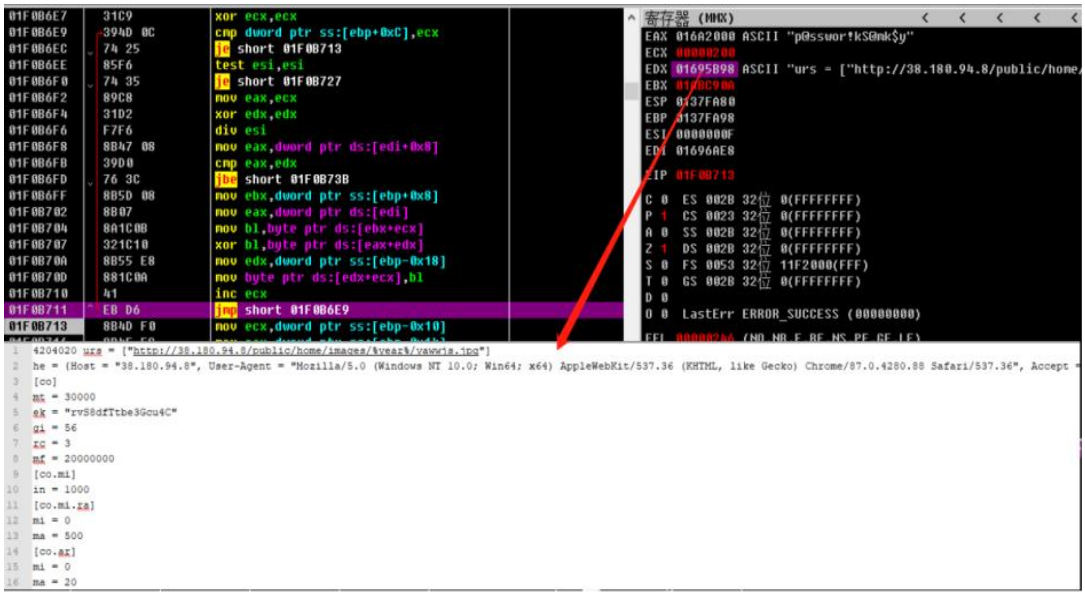


String	Address	Type	Codec	Tag	C...	S...
110NgaeSkmTOI4EykC3dQTO3ohKxvOhC4qhY...r9qTcYIfcesUA/oN0b56NkEtI9elnuUIOGJ	0x0233f965 (:233f965)	SCAN	Ascii	BASE64	2...4	139
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx...xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	0x00cea145 (:cea145)	SCAN	Ascii		63488	95
Windows Registry Editor Version 5.00...0.00.00.01.00.00.00.01.00.00.00/s/s	0x04f25e27 (:4f25e27)	SCAN	Utf16		59230	102
.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx...xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	0x01f3bf1e (:1f3bf1e)	SCAN	Ascii		55047	95
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx...xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	0x00cdc251 (:cdc251)	SCAN	Ascii		55020	95
Windows Registry Editor Version 5.00... 00.00.00.00.00.00.00.01.00.00.00/s	0x04f71517 (:4f71517)	SCAN	Utf16		54233	101

经过两个阶段的 shellcode 执行后，在内存中展开名为 client.dll 的库文件并执行其中的代码，该文件的详细信息如下：

描述	详细信息
名称	Client.dll
文件大小	1684480 bytes
文件类型	RUST
文件功能	RAT
编译时间	/
开发平台及语言	/
是否加壳	否
VT 首次上传时间	2023-03-08 11:05:03 UTC
md5	d2a6b4906326311c221a77c805bdfa8a
Sha256	4f7d2738cc40493bded2e7acca155274c67258d5072c e44220b3cc2ba4afc63c

该文件是由 RUST 编写的远控程序，实现了远程命令执行、文件窃取、文件下载、文件执行、远程代码执行等功能。使用密钥“p@sswor!kS@mk$y”异或解密附加在文件尾部的数据，得到配置数据。



远程命令执行使用的是传统的重定向 cmd 进程的输入输出流到管道中，管道的另一边通过网络通信与攻击者的服务器连接，攻击者在服务器输入的命令都能通过管道传输到 cmd 中执行并回显执行结果。

文件执行时，当文件不存在，则下载文件到%temp%路径下，然后再调用 ShellExecute 执行文件。

```
  }
  goto LABEL_292;
case 7:                                 // 文件执行，当文件不存在时就写入文件再执行
  dwMajorVersion = v237[8];
  LODWORD(v232) = v237[6];
  if ( v237[5] == 1 )
  {
    sub_10007018((unsigned int *)v281, v237 + 9);
    if ( v281[0].m128i_i32[0] )
    {
      p_VersionInformation = (struct _OSVERSIONINFOW *)v281[0].m128i_i32[2];
      *(_QWORD *)&VersionInformation.dwOSVersionInfoSize = v281[0].m128i_i64[0];
      VersionInformation.dwMinorVersion = v281[0].m128i_u32[2];
      v35 = v281[0].m128i_i32[0];
    }
    else
    {
      v35 = 1;
      p_VersionInformation = 0;
      VersionInformation.dwOSVersionInfoSize = 1;
      VersionInformation.dwMajorVersion = 0;
      VersionInformation.dwMinorVersion = 0;
    }
    sub_10027391(v232, (int)nSize, dwMajorVersion, v35, (int)p_VersionInformation)
    v104 = &VersionInformation;
L_291:
    sub_10048D8C(v104);
    LOBYTE(v15) = nSize[0];
    if ( LOBYTE(nSize[0]) != 8 )
    {
      v14 = DWORD2(nSize[0]);
      HIDWORD(v232) = DWORD2(nSize[1]);
      v12 = DWORD1(nSize[1]);
      dwMajorVersion = (BYTE3(nSize[0]) << 16) | *(unsigned __int16 *)((char *)nSize + 1);
      dwMinorVersion = HIDWORD(nSize[1]);
```

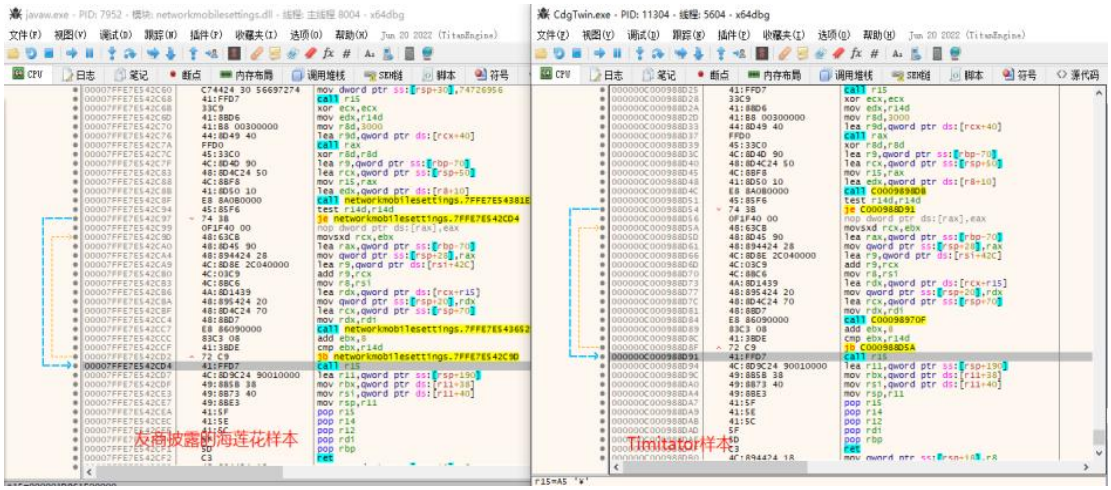
```
  v22 = a2;
  v19 = v15;
  v20 = v16[0];
  sub_100274AD(HIDWORD(v16[0]));
  sub_100274AD(4);
  sub_100274AD(v17);
  ShellExecuteW(0, (LPCWSTR)v18[0], (LPCWSTR)v21[0], (LPCWSTR)v17[0], (LPCWSTR)v17[0], 0);
  sub_100C9A65((char *)v16 + 4, LastError);
  LOBYTE(v15) = 0;
  LODWORD(v16[0]) = LastError;
  v11 = v16[0];
  v12 = v15;
  v13 = v22;
  *(_QWORD *)(v22 + 16) = v16[1];
  *(_QWORD *)(v13 + 8) = v11;
  sub_100C6A58((int *)v17);
  sub_100C6A58((int *)v18);
  sub_100C6A58((int *)v21);
  *(_BYTE *)v13 = 5;
  *(_DWORD *)(v13 + 4) = v12;
  return sub_10048D8C(&v19);
}
return result;
```

远程代码执行，根据提供的文件名，将文件数据复制到可执行内存中，随后创建线程执行。

```
case 8:                                 // 申请内存，创建线程执行
  if ( v237[5] == 1 )
    sub_10027545(v237[6], (int)v281, v237[8]);// 读文件
  else
    sub_100276E6(v237[6], (int)v281, v237[8]);
  dwMajorVersion = v281[0].m128i_i32[1];
  *(_DWORD *)v219 = v281[0].m128i_i32[3];
  if ( v281[0].m128i_i32[0] != 1 )
  {
    p_VersionInformation = &VersionInformation;
    *(_QWORD *)&VersionInformation.dwOSVersionInfoSize = *(__int64 *)((char *)v281[0].m128i_i64 + 4);
    VersionInformation.dwMinorVersion = v281[0].m128i_u32[3];
    sub_10008992(&VersionInformation, 195);
    dwMajorVersion = VersionInformation.dwMinorVersion;
    v281[0].m128i_i32[2] = VersionInformation.dwMinorVersion;
    v281[0].m128i_i64[0] = *(_QWORD *)&VersionInformation.dwOSVersionInfoSize;
    v52 = (struct _OSVERSIONINFOW *)VirtualAlloc(0, VersionInformation.dwMinorVersion, 0x3000u, 0x40u);
    if ( v52 )
    {
      p_VersionInformation = v52;
      sub_100CC480((unsigned int)v52, v281[0].m128i_u32[0], dwMajorVersion);
      LODWORD(nSize[0]) = 0;
      CreateThread(0, 0x400000u, (LPTHREAD_START_ROUTINE)p_VersionInformation, 0, 0, (LPDWORD)nSize);
    }
    sub_10048D8C(v281);
    goto LABEL_292;
  }
  p_VersionInformation = (struct _OSVERSIONINFOW *)v281[1].m128i_i32[3];
  v12 = v281[1].m128i_i32[2];
  *(_QWORD *)&v219[4] = v281[1].m128i_i64[0];
  dwMinorVersion = v281[2].m128i_u32[0];
```

3 关联分析

在分析中我们发现样本中提取到的 shellcode 与近期友商披露的海莲花样本中使用的高度一致，下图展示的是第一阶段的 shellcode，第二阶段的 shellcode 也是基本一致。



此外不仅是攻击时偏爱使用 CobaltStrike，在提取到的 CobaltStrike 配置信息中的，使用的域名结构为*-*-*，cloudflare 服务。

文件 hash	C2
4a8756b22029a88506744ab7864c9b83	strengthening-memories-reportsrestoration.trycloudflare.com

友商披露的样本。

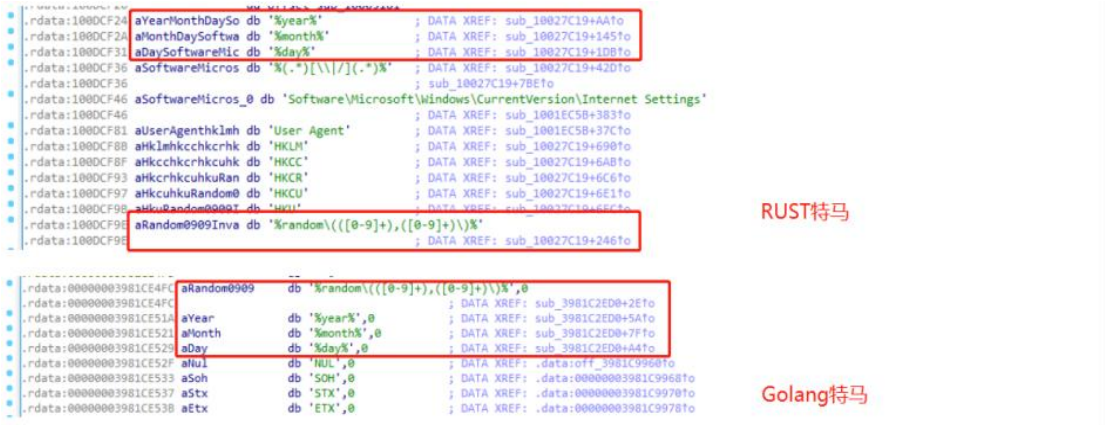
文件 hash	C2
064cd0afb4dc27df9d30c7f5209a8e5b	oo-advances-computers-interests.trycloudflare.com
3ada3a7ff12dbe5e129b4aec77051843	guilty-patricia-connecticut-pulled.trycloudflare.com

无独有偶，这批样本并不是 Timitator 第一次使用特马，在 2023 年，我们就观测到该组织使用的 golang 特马。

sha256	上传时间	Filetype	C2
38c815370bddf0e1d0552801de06e544c6656171b0d1435c3dc66d3ac3bcdd2a	2023-02-15	ELF	185.32.126.126:5353
6c959ea4fd3b4dcf8202237870e0782a18bfde05418157b42377c9475355d3ac	2023-12-21	ELF	129.232.134.106:443
774c9181a53d08b245a71a2cf7f55c24c4dbc7fa5e4b7e0aa39f855c74c65e55	2024-02-01	DLL	45.131.132.146:80

二者都是由同一份代码编译出来的，分别运行在 linux 和 windows 平台。

在与 RUST 特马的字符串特征比较中，疑似出自同一位开发者。



4 总结

Timitator 组织仍处于活跃状态仍需警惕来自该组织的定向攻击。不过此前他们多次使用 CobaltStrike，而 CobaltStrike 本是各家安全厂商关注的重点，因此该组织正在寻求隐秘性更高的远控程序和攻击技术来应对安全软件的围追堵截，使用自定义特马是他们做出的改变。同时在钓鱼文件添加更高可信度的描述信息，带着伪装的文件签名则是为了更好地迷惑用户，增加钓鱼的成功率。

深信服蓝军高级威胁（APT）团队专注全球高级威胁事件的跟踪与分析，拥有一套完善的自动化分析溯源系统以及外部威胁监控系统，能够快速精准地对 APT 组织使用的攻击样本进行自动化分析和关联，同时积累并完善了几十个 APT 以及网络犯罪威胁组织的详细画像，成功帮助客户应急响应处置过多起 APT 及网络犯罪威胁组织攻击事件，未来随着安全对抗的不断升级，威胁组织会研究和使用更多新型的 TTP，深信服高级威胁团队会持续监控，并对全球发现的新型安全事件进行深入分析与研究。

5 IOC

IOC 类型	详细信息
IP:PORT	39.104.205.68:443
IP:PORT	38.180.94.8:80
IP:PORT	64.176.58.16:80
IP:PORT	207.148.71.4:443
IP:PORT	129.232.134.106:443
IP:PORT	45.131.132.146:80
DOMAIN	strengthening-memories-reports-restoration.trycloudflare.com:443
SHA256	49d3777d0d02cd2a4d1c44313c72279fee1681c1e3566535f9117d17b274424b
SHA256	acf0fb4dac33e197de3a3e142eeaa7e5a892607424e8ea8708d49c65f3703d61
SHA256	87bfce678855fa498d85b143beaf129f9bd468ebdcc1226b2ba39780a02f3d2e

SHA256	aac2cbd4cb119dec6c9a8c58f86b8bdd83d27fdaed85149bb2572599de9e32c0
SHA256	6c959ea4fd3b4dcf8202237870e0782a18bfde05418157b42377c9475355d3ac
SHA256	774c9181a53d08b245a71a2cf7f55c24c4dbc7fa5e4b7e0aa39f855c74c65e55
SHA256	ba27c022b5e81fc719ed3097f950bb3e7613dc2c8b9b2851bbb573f7c48ae286
SHA256	6cb80b939b8de9f15726391f807b947951083da28c2647b8c8451021d559f7ee

参考链接

https://mp.weixin.qq.com/s/K-FUaffQx4g6d_hweXxCTg

三、安全热点

（一）伦敦证券旗下数据库被窃取，泄露超 500 万条敏感信息

5 月 5 日消息，一名自称 GhostR 的攻击者宣称，成功窃取并泄露了伦敦证券交易所集团（LSEG）旗下 World-Check 数据库。该数据库中存储了超 500 万条关于政治公众人物、罪犯、风险组织以及其他机构的数据信息。根据攻击者提供的泄露数据样本，World-Check 原始数据信息包括社会安全号码、银行账号、加密货币账户、护照、出生日期和工作地点等。LSEG 是全球领先的金融市

场基础设施提供商，为 170 多个国家/地区的 4 万多名客户提供金融数据、分析、新闻和指数产品。LSEG 在声明中透露，World-Check 数据库泄露事件不涉及公司其它网络系统，目前正与客户联系并通知有关当局。（信息来源：FreeBuf 网）

（二）超 5 万台 Tinyproxy 服务器易受严重 RCE 漏洞影响

5 月 9 日消息，攻击面管理公司 Censys 发现超 5 万台暴露在互联网的 Tinyproxy 服务器易受 RCE 漏洞 CVE-2023-49606（CVSS 评分 9.8）影响，大多数设备位于美、中、韩等国。该漏洞位于“remove_connection_headers()”函数中，攻击者无需认证，即可通过一个简单的恶意 HTTP 请求利用该漏洞，可能导致内存被释放且遭不恰当访问，影响 1.11.1 和 1.10.0 版本。Tinyproxy 是一款开源的 HTTP 和 HTTPS 代理服务器，常用于小型企业、公共 WiFi 提供商和家庭用户。该公司尚未发布补丁。（信息来源：FreeBuf 网）

（三）英国防部超 22.5 万名军事人员信息遭泄露

5 月 9 日消息，一家为英国防部提供薪资处理服务的企业遭网络攻击，其处理系统中超 22.5 万名英国陆军、海军和皇家空军现役军人、预备役军人和退役军人的个人姓名、银行账号等详情信息被访问。英国媒体确认外部承包商为 Shared Services Connected Ltd，并表示被入侵的薪资系统还包含多年前的军事人员信息。英国防大臣格兰特·沙普斯指出，此次攻击很可能得到了民族国家的支持，指责第三方承包商未能充分保护系统。（信息来源：环球时报）

四、网络安全政策法律动态

（一）中央网信办等四部门印发《2024 年数字乡村发展工作要点》

中央网信办等四部门印发《2024年数字乡村发展工作要点》

2024年05月15日 21:15　来源：中国网信网　【打印】【纠错】

近日，中央网信办、农业农村部、国家发展改革委、工业和信息化部联合印发《2024年数字乡村发展工作要点》。通知要求，深入贯彻落实习近平总书记关于乡村振兴的重要指示批示精神和中央经济工作会议、中央农村工作会议精神，认真落实《中共中央 国务院关于学习运用“千村示范、万村整治”工程经验 有力有效推进乡村全面振兴的意见》（中发〔2024〕1号）部署要求，深入实施《数字乡村发展战略纲要》《数字乡村发展行动计划（2022—2025年）》，以信息化驱动引领农业农村现代化，促进农业高质高效、乡村宜居宜业、农民富裕富足，为加快建设网络强国、农业强国提供坚实支撑。

《工作要点》明确了工作目标：到2024年底，数字乡村建设取得实质性进展。数字技术保障国家粮食安全、巩固拓展脱贫攻坚成果更加有力。农村宽带接入用户数超过2亿，农村地区互联网普及率提升2个百分点，农产品电商网络零售额突破6300亿元，农业生产信息化率进一步提升，培育一批既懂农业农村、又懂数字技术的实用型人才，打造一批示范性强、带动性广的数字化应用场景，抓好办成一批线上线下联动、群众可感可及的实事。

《工作要点》部署了9个方面28项重点任务。**一是筑牢数字乡村发展底座。**包括提升农村网络基础设施供给能力，加大农村基础设施改造升级力度，加快推进涉农数据资源集成共享。**二是以数字化守牢“两条底线”。**包括强化确保粮食安全数字化支撑，强化防止返贫监测和帮扶举措。**三是大力推进智慧农业发展。**包括加强农业科技创新与应用推广，提升农业全产业链数字化水平，以数字技术深化农业社会化服务。**四是激发县域数字经济新活力。**包括加快推进农村电商高质量发展，多措并举推动农文旅融合发展，释放涉农数据要素乘数效应，运用数字技术促进农民增收。**五是推动乡村数字文化振兴。**包括加快乡村文化文物资源数字化，丰富乡村公共文化服务数字供给。**六是健全乡村数字治理体系。**包括稳步推进农村“三务”信息化建设，提升农村社会治理数字化效能，增强农村智慧应急管理能力。**七是深化乡村数字普惠服务。**包括着力提升乡村教育数字化水平，持续推进乡村数字健康发展，增强农村数字普惠金融服务实效，加强农村特殊人群信息服务保障。**八是加快建设智慧美丽乡村。**包括加强农村人居环境整治数字化应用，提升农村生态环境保护监管效能。**九是统筹推进数字乡村建设。**包括加强跨部门跨层级协调联动，健全多元化投入保障机制，培养壮大乡村数字人才队伍，推进重点领域标准化建设，讲好新时代数字乡村故事。

NEWS 相关链接

2024年数字乡村发展工作要点

参考链接：

https://www.cac.gov.cn/2024-05/15/c_1717449025941328.htm

（二）关于 16 项网络安全国家标准获批发布的通知

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of Standardization Administration of China

搜索

首页 | 工作动态 | 行业观点 | 标准征求意见 | 标准查询 | 出版物 | 关于我们 | 平台登录

通知公告

关于16项网络安全国家标准获批发布的通知

2024-05-09

根据2024年4月25日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024年第6号），全国网络安全标准化技术委员会归口的16项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 18336.1—2024	网络安全技术 信息技术安全评估准则 第1部分：简介和一般模型	GB/T 18336.1—2015	2024-11-1
2	GB/T 18336.2—2024	网络安全技术 信息技术安全评估准则 第2部分：安全功能组件	GB/T 18336.2—2015	2024-11-1
3	GB/T 18336.3—2024	网络安全技术 信息技术安全评估准则 第3部分：安全保障组件	GB/T 18336.3—2015[部]	2024-11-1
4	GB/T 18336.4—2024	网络安全技术 信息技术安全评估准则 第4部分：评估方法和活动的规范框架	GB/T 18336.3—2015[部]	2024-11-1
		网络安全技术 信息技术安全	GB/T 18336.3—	

参考链接：

https://www.tc260.org.cn/front/postDetail.html?id=20240509163346

五、微软安全通告

（一） 漏洞概要

2024 年 5 月 15 日（北京时间），微软发布了安全更新，共发布了 63 个 CVE 的补丁程序，同比上月减少了 92 个。

在漏洞安全等级方面，存在 1 个标记等级为“Critical”的漏洞，61 个漏洞被标记为“Important/High”等级的漏洞；在漏洞类型方面，主要有 29 个远程代码执行漏洞，17 个权限提升漏洞以及 7 个信息泄露漏洞。

（二） 漏洞数据分析

1 漏洞数量趋势

2024 年微软补丁漏洞修复情况

总体上来看，微软本月发布的补丁数量为 63 个，有 1 个 Critical 漏洞补丁。

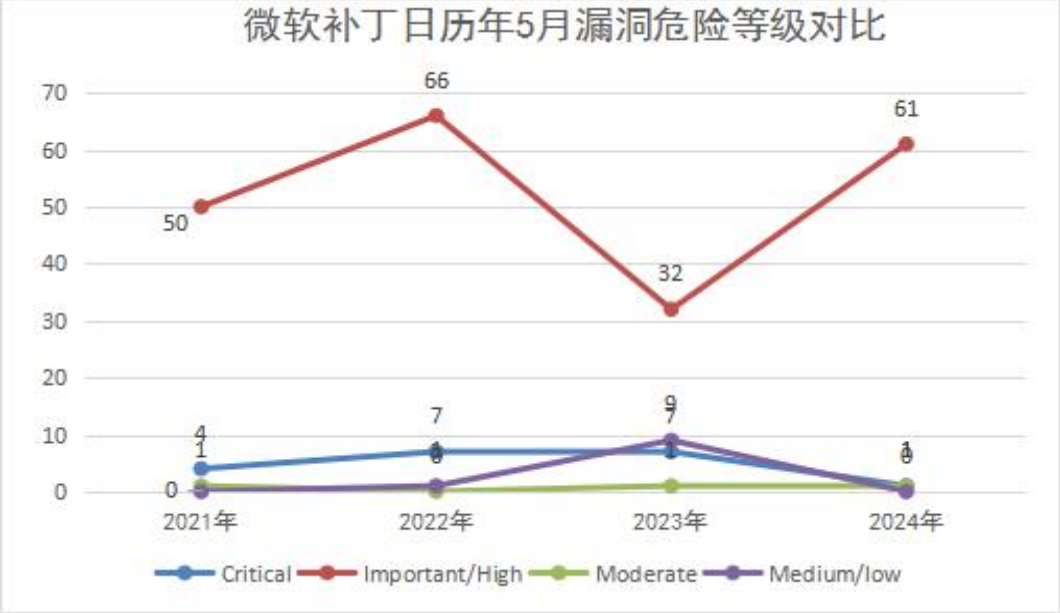
千里目安全技术中心在综合考虑往年微软公布漏洞数量的数据统计和今年的特殊情况，初步估计微软在今年六月份公布的漏洞数将比今年五月份多。漏洞数量将会维持在 75 个左右。

2 历史微软补丁日 5 月漏洞对比

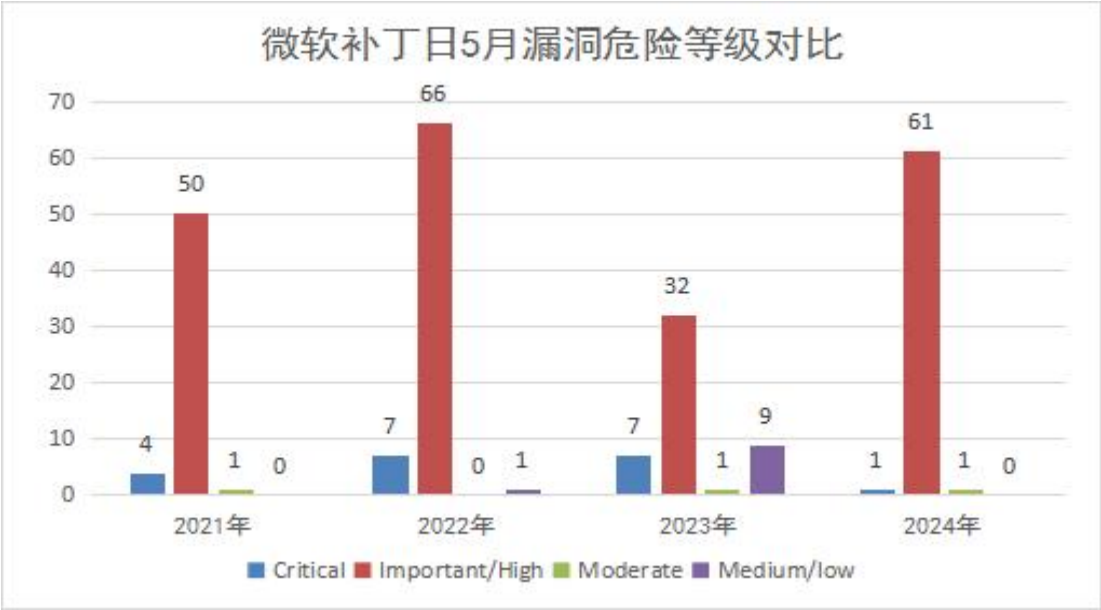
2021-2024 年，5 月份的漏洞数趋势如下图：

历年 5 月份微软 Windows 补丁趋势

2021—2024 年，5 月份的漏洞危险等级趋势和数量如下图：

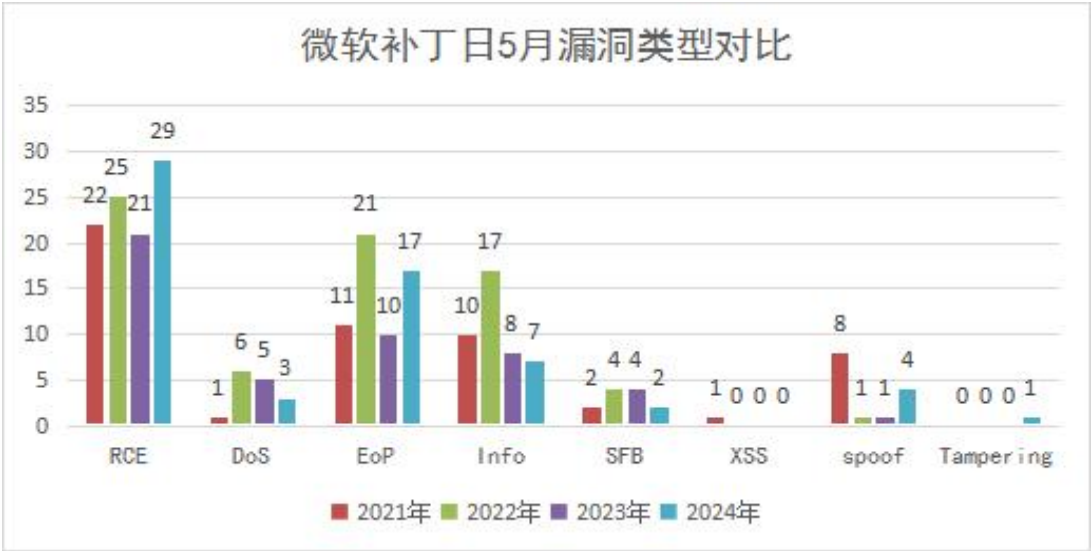


历年 5 月份微软漏洞趋势



历年 5 月份微软漏洞危险等级对比

2021—2024 年，5 月份的漏洞各个类型数量对比如下图：



微软近年 5 月漏洞类型对比

3 漏洞数量分析

从漏洞数量来看，今年相较去年增多。微软在 2024 年 5 月份爆发的漏洞相较于去年增多。本月出现了 63 个漏洞补丁，并且有 1 个 Critical 类型的漏洞补丁。

从漏洞的危险等级来看，相较去年“Critical”等级的漏洞数量减少，“Important/High”等级的漏洞数量增多。本月出现了 1 个“Critical”等级的漏洞，相较去年减少了约 86%；本月出现了 61 个“Important/High”等级的漏洞，相较去年增加了约 91%。

从漏洞类型来看，RCE 类型的漏洞数量增多，DoS 类型的漏洞数量减少，EoP 类型的漏洞数量增多，仍然需要引起高度重视，尤其是 RCE 漏洞在配合社工手段的前提下，甚至可以直接接管整个局域网并进行进一步扩展攻击。

（三） 重要漏洞分析

1 漏洞分析

Windows DWM 核心库特权提升漏洞 CVE-2024-30051

DWM 桌面窗口管理器是自 Windows Vista 以来 Microsoft Windows 中的合成窗口管理器，它允许使用硬件加速来呈现 Windows 的图形用户界面。它最初是为了启用部分新的“ Windows Aero ”用户体验而创建的，它允许诸如透明度、3D 窗口切换等效果。

其中存在特权提升漏洞，攻击者可以利用该漏洞在目标系统上获取更高的权限。漏洞存在在野利用，经过评估，危害比较大，我们建议用户及时更新微软安全补丁。

Windows MSHTML 平台安全功能绕过漏洞 CVE-2024-30040

MSHTML 提供了一个 COM 接口，用于在任何支持 COM 的环境（如 C++和.NET）中访问和编辑网页。

其中存在安全功能绕过漏洞，攻击者可以利用该漏洞在绕过目标系统上的安全功能，做出规定之外的行为。漏洞存在在野利用，经过评估，危害比较大，我们建议用户及时更新微软安全补丁。

2 影响范围

漏洞名称/CVE	受影响版本
Windows DWM 核心库特权提升洞 CVE-2024-30051	Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 (Server Core installation)

	Windows Server 2022 Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems
Windows SHTML 平台安全功能绕过漏洞 CVE-2024-30040	Windows Server 2022 Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016

	Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 version 21H2 for ARM64-based Systems

	Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2016 (Server Core installation) Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems

3 修复建议

微软官方已更新受影响软件的安全补丁，用户可根据不同系统版本下载安装对应的安全补丁。

安全更新链接如下：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040

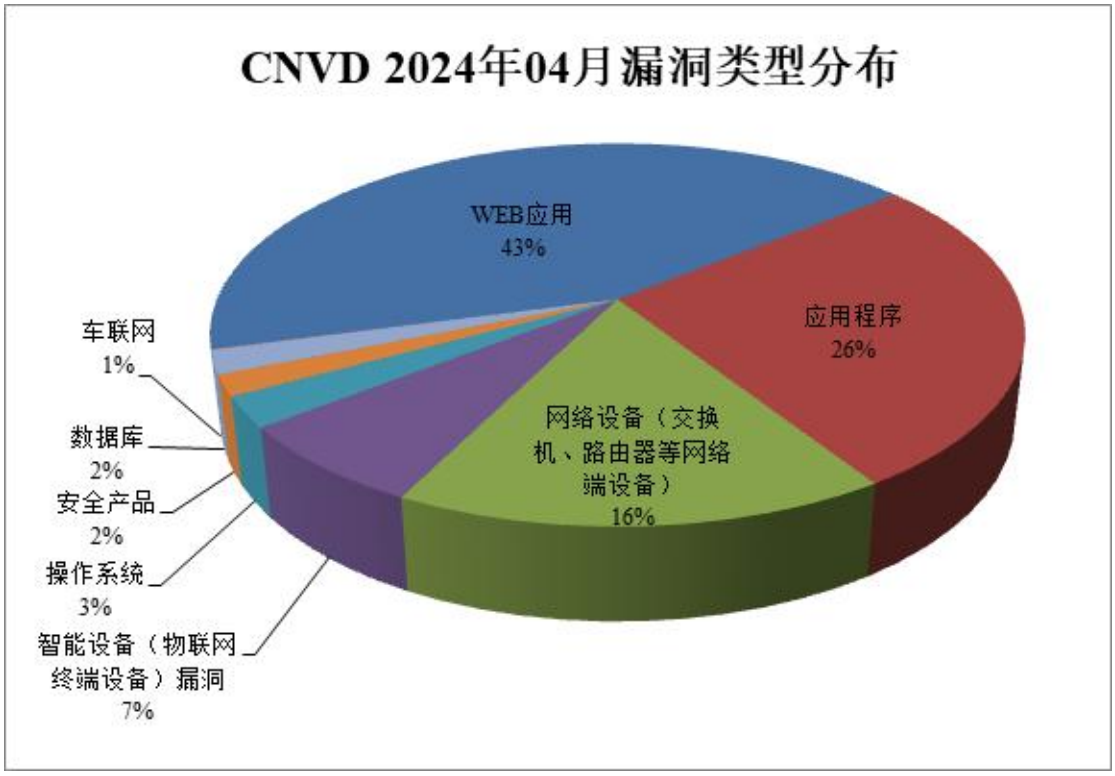
六、CNVD 漏洞收录情况

国家信息安全漏洞共享平台（China National Vulnerability Database，以下简称 CNVD），4 月收集整理信息安全漏洞 2350 个，其中高危漏洞 907 个，中危漏洞 1370 个，低危漏洞 73 个。

上述漏洞中，可被利用来实施远程网络攻击的漏洞有 2174 个，数据来源自 CNVD 站点漏洞统计数据。

（一）漏洞分类统计

根据漏洞影响对象的类型，漏洞可分为 WEB 应用、应用程序、操作系统、网络设备（交换机、路由器等网络端设备）、数据库、安全产品（如防火墙、入侵检测系统等）、车联网和智能设备（物联网终端设备）漏洞。不同类型漏洞的分布如图 1 所示，本月 WEB 应用占比例较大。与前 12 个月相比，本月应用程序、WEB 应用、数据库、网络设备（交换机、路由器等网络端设备）、安全产品、智能设备（物联网终端设备）漏洞的数量处于高位，操作系统、车联网漏洞的数量处于低位。



漏洞类型分布

（二）漏洞关注情况

根据对用户查阅CNVD漏洞信息次数的统计，4月用户关注的主要是Tenda AC10 缓冲区溢出漏洞（CNVD-2024-20301），其访问量达到 22 次以上，关注度最高的 5 个漏洞如下。

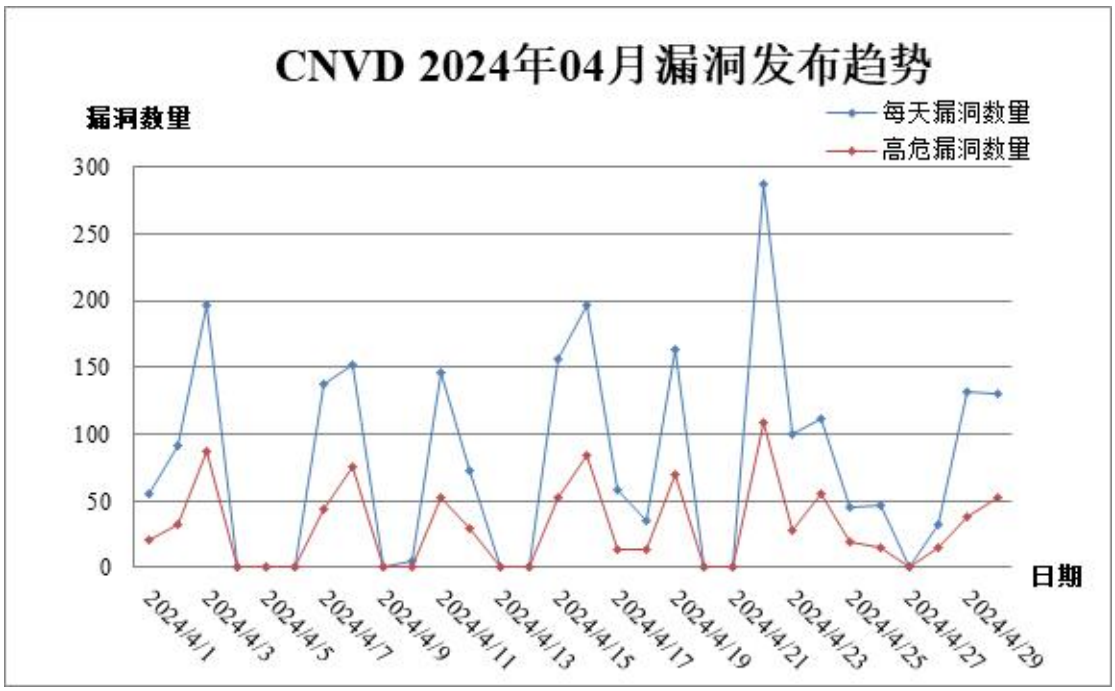
关注度排名	漏洞名称	CNVD 编号	发布时间
1	Tenda AC10 缓冲区溢出漏洞（CNVD-2024-20301）	CNVD-2024-20301	2024/4/12
2	Online Courseware editt.php 文件跨站脚本漏洞	CNVD-2024-20289	2024/4/12

3	Tenda W18E 缓冲区溢出漏洞	CNVD-2024-20280	2024/4/12
4	Tenda AX1803 serviceName 参数缓冲区溢出漏洞	CNVD-2024-20293	2024/4/12
5	Tenda FH1205 命令注入漏洞	CNVD-2024-20298	2024/4/12

4 月被关注漏洞 Top5

（三）漏洞趋势

4 月，CNVD 收集整理信息安全漏洞 2350 个，与前 12 个月平均收录数量 1726 个相比，处于高位；本月高危漏洞 907 个，与前 12 个月高危漏洞平均收录数量 767 个相比，处于高位。4 月 22 日发布的安全漏洞数量最多，高达 288 个，主要是因为收录了 Oracle、IBM 等多款产品存在的多个漏洞。4 月的总体漏洞发布趋势如图所示：


CNVD 2024年04月漏洞发布趋势
漏洞数量
每天漏洞数量
高危漏洞数量
300
250
200
150
100
50
0
日期
2024/4/1
2024/4/3
2024/4/5
2024/4/7
2024/4/9
2024/4/11
2024/4/13
2024/4/15
2024/4/17
2024/4/19
2024/4/21
2024/4/23
2024/4/25
2024/4/27
2024/4/29

4 月份漏洞发布趋势

附录：4 月份重要漏洞信息汇总

4 月份对国内用户广泛使用的信息系统和应用程序影响较大的重要漏洞如下表所示。

序号	漏洞名称	编号及影响产品信息		影响描述
1	Microsoft 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-17975、CNVD-2024-17976CNVD-2024-19326、CNVD-2024-19327CNVD-2024-19328、CNVD-2024-19329CNVD-2024-19330、CNVD-2024-19331CNVD-2024-19332、CNVD-2024-19333	本月，Microsoft 多款产品存在安全漏洞。攻击者可利用该漏洞导致拒绝服务，升级权限，在系统上执行任意代码等。本月漏洞包括：Microsoft Edge (Chromium-based)信息泄露漏洞 (CNVD-2024-17975) 、Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-17976）、Microsoft Windows
		其他编号	CVE-2024-26192、CVE-2024-21399 CVE-2024-21408、CVE-2024-21407 CVE-2024-21323、CVE-2024-29053 CVE-2024-29054、CVE-2024-29055 CVE-2024-26257、CVE-2024-290	

			64	Hyper-V 拒绝服务漏洞（CNVD-2024-19326、CNVD-2024-19333）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2024-19327）、Microsoft Defender for IoT 远程代码执行漏洞（CNVD-2024-19328、CNVD-2024-19329）、Microsoft Defender for IoT 权限提升漏洞（CNVD-2024-19330、CNVD-2024-19331）、Microsoft Excel 远程代码执行漏洞（CNVD-2024-19332）等。
		发布时间	2024-04-25	
		影响产品	Microsoft Edge (Chromium-based) Microsoft Window 10 Microsoft Window 11 Microsoft Windows Server 2022 Microsoft Windows Server 2012 Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Defender for IoT Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Office LTSC for Mac 2021	
2	Google 多	**CNVD 编**	CNVD-2024-16875、CNVD-2024	本月，Google 多款

	款产品存在安全漏洞	**号**	-16876CNVD-2024-16879、CNVD-2024-16880CNVD-2024-16881、CNVD-2024-16882CNVD-2024-16883、CNVD-2024-16894CNVD-2024-16936、CNVD-2024-16937	产品存在安全漏洞。攻击者可利用该漏洞获取敏感信息，绕过安全限制，在系统上执行任意代码等。本月漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2024-16936、CNVD-2024-16881、CNVD-2024-16875）、Google Chrome 代码执行漏洞（CNVD-2024-16876、CNVD-2024-16880、CNVD-2024-16937）、Google Android 代码执行漏洞(CNVD-2024-16883)、Google Android 权限提升漏洞（CNVD-2024-16894、C
		其他编号	CVE-2024-2630、CVE-2024-2625 CVE-2024-2626、CVE-2024-2627 CVE-2024-2628、CVE-2024-23717 CVE-2024-0039、CVE-2022-42531 CVE-2024-1672、CVE-2024-1673	
		发布时间	2024-04-12	
		影响产品	Google Android Google Chrome	

				NVD-2024-16882)、Google Chrome 信息泄露漏洞 (CNVD-2024-16879) 等。
3	IBM 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-15726、CNVD-2024-15728 CNVD-2024-15731、CNVD-2024-18059 CNVD-2024-19019、CNVD-2024-19025 CNVD-2024-20492、CNVD-2024-20497 CNVD-2024-20821、CNVD-2024-20840	本月，IBM 多款产品存在安全漏洞。攻击者可利用该漏洞获取高度敏感的私有信息，发送特制的 SQL 语句，从而允许攻击者查看、添加、修改或删除后端数据库中的信息，提交特殊的请求，可以应用程序上下文执行任意代码等。本月漏洞包括：IBM QRadar SIEM 跨站脚本漏洞 (CNVD-2024-15726) 、IBM Common Cryptogra
		其他编号	CVE-2023-50961、CVE-2023-47150 CVE-2022-43842、CVE-2024-22353 CVE-2024-31887、CVE-2024-28787 CVE-2024-31871、CVE-2024-223	

			28 CVE-2024-31873、CVE-2024-25029	phic Architecture 资源管理错误漏洞、IBM Aspera SQL 注入漏洞、IBM WebSphere Application Server Liberty 资源管理错误漏洞（CNVD-2024-18059）、IBM Security Verify Privilege 信息泄露漏洞、IBM Security Verify Access Appliance和IBM Application Gateway 信息泄露漏洞、IBM Security verify Access Appliance 信任管理问题漏洞、IBM Maximo Application Suite 目录遍历漏洞、IBM Security
		发布时间	2024-04-17	
		影响产品	IBM QRadar SIEM IBM Common Cryptographic Architecture IBM Aspera IBM WebSphere Application Server Liberty IBM Security Verify Privilege IBM Security verify Access Appliance IBM Security Verify Access IBM Application Gateway IBM maximo application suite IBM Personal Communications	

				Verify Access 信任管理问题漏洞（CNVD-2024-20821）、IBM Personal Communications 任意代码执行漏洞等。
4	Cisco 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-20825、CNVD-2024-20824CNVD-2024-20823、CNVD-2024-20830CNVD-2024-20829、CNVD-2024-20828CNVD-2024-20827、CNVD-2024-20826CNVD-2024-20832、CNVD-2024-20831	本月，Cisco 多款产品存在安全漏洞。攻击者可利用该漏洞获取敏感信息，注入精心设计的有效载荷执行任意 Web 脚本或 HTML，获得对受影响设备上的文件系统或托管容器的 root 访问权限等。本月漏洞包括：Cisco Enterprise Chat and Email 跨站脚本漏洞、Cisco Emergency Responder 目录遍历漏洞（CN
		其他编号	CVE-2024-20367、CVE-2024-20352 CVE-2024-20347、CVE-2024-20362 CVE-2024-20283、CVE-2024-20282 CVE-2024-20302、CVE-2024-20332 CVE-2024-20310、CVE-2024-203	

			34	VD-2024-20824）、Cisco Emergency Responder 跨站请求伪造漏洞、Cisco Small Business 跨站脚本漏洞、Cisco Nexus Dashboard 信息泄露漏洞、Cisco Nexus Dashboard 权限提升漏洞、Cisco Nexus Dashboard 访问控制错误漏洞（CNVD-2024-20827）、Cisco Identity Services Engine 服务器端请求伪造漏洞、Cisco Unified Communications Manager 跨站脚本漏洞（CNVD-2024-20832）、Cisco TelePresence
		发布时间	2024-04-12	
		影响产品	Cisco RV320 Cisco RV325 Cisco RV016 Cisco RV042 Cisco RV042G Cisco RV082 Cisco Nexus Dashboard Cisco Identity Services Engine Cisco Unified Communications Manager Cisco TelePresence Management Suite Cisco Enterprise Chat and Email Cisco Emergency Responder	

				Management Suite 跨站脚本漏洞（CNVD-2024-20831）等。
5	Apache 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-16107、CNVD-2024-16106 CNVD-2024-16110、CNVD-2024-16109 CNVD-2024-17935、CNVD-2024-17934 CNVD-2024-17933、CNVD-2024-17932 CNVD-2024-17938、CNVD-2024-17937	本月，Apache 多款产品存在安全漏洞。攻击者可利用该漏洞使用 sqlSearch 参数发送特制的 SQL 语句，查看、添加、修改或删除后端数据库中的信息，发送特制的请求，在系统上执行任意代码等。 本月漏洞包括：Apache Fineract SQL 注入漏洞（CNVD-2024-16107、CNVD-2024-16106）、Apache Commons Configuration 越界写入漏洞（CNVD-2
		其他编号	CVE-2024-23538、CVE-2024-23539 CVE-2024-29131、CVE-2024-29133 CVE-2024-31862、CVE-2024-31860 CVE-2024-31866、CVE-2024-31863	

			CVE-2024-31864、CVE-2024-31867	024-16109、CNVD-2024-16110、CNVD-2024-16110）、Apache Zeppelin 代码执行漏洞、Apache Zeppelin 安全绕过漏洞、Apache Zeppelin 代码注入漏洞（CNVD-2024-17938）、Apache Zeppelin 输入验证错误漏洞（CNVD-2024-17937、CNVD-2024-17935、CNVD-2024-17934）等。
		发布时间	2024-04-17	
		影响产品	Apache Fineract Apache Commons Configuration Apache Zeppelin	
6	Foxit 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-16874、CNVD-2024-17005CNVD-2024-17009、CNVD-2024-17008CNVD-2024-17007、CNVD-2024-17006CNVD-2024-17012、CNVD-2024-17010CNVD-2024-20599、CNVD-2024-20	本月，Foxit 多款产品存在安全漏洞。攻击者可利用该漏洞写入任意文件，提交特殊的文件请求，诱使用户解析，可使应

			601	用程序崩溃或以应用程序上下文执行任意代码等。本月漏洞包括：Foxit PDF Reader 和 PDF Editor 代码执行漏洞、Foxit PDF Reader Doc Object 代码执行漏洞、Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2024-17009）、Foxit PDF Reader 远程代码执行漏洞（CNVD-2024-17008）、Foxit PDF Reader AcroForm 代码执行漏洞（CNVD-2024-17006、CNVD-2024-17007）、Foxit Reader 和 Foxit PhantomPDF 任意文件
		其他编号	CVE-2024-25858、CVE-2024-30338 CVE-2022-24908、CVE-2024-30371 CVE-2024-30367、CVE-2024-30365 CVE-2021-38573、CVE-2021-41785 CVE-2024-30330、CVE-2024-30328	
		发布时间	2024-04-09	
		影响产品	Foxit PDF Editor Foxit PDF Reader Foxit PhantomPDF Foxit Reader	

				写入漏洞、Foxit PDF Reader and Foxit PDF Editor 缓冲区溢出漏洞、Foxit PDF Reader代码执行漏洞（CNVD-2024-20601、CNVD-2024-20599）等。
7	Oracle多款产品存在安全漏洞	**CNVD编号**	CNVD-2024-19011、CNVD-2024-19010CNVD-2024-19009、CNVD-2024-19014CNVD-2024-19013、CNVD-2024-19012CNVD-2024-19018、CNVD-2024-19017CNVD-2024-19016、CNVD-2024-19015	本月，Oracle 多款产品存在安全漏洞。攻击者可利用该漏洞导致 MySQL 服务器挂起或频繁重复崩溃等。本月漏洞包括：Oracle MySQL 拒绝服务漏洞（CNVD-2024-19011、CNVD-2024-19010、CNVD-2024-19009、CNVD-2024-19014、CNVD-2024-19013、CNVD-202
		其他编号	CVE-2024-20994、CVE-2024-21008 CVE-2024-21062、CVE-2024-21052 CVE-2024-21055、CVE-2024-21056 CVE-2024-21013、CVE-2024-210	

			09 CVE-2024-21049、CVE-2024-21051	4-19012、CNVD-2024-19018、CNVD-2024-19017、CNVD-2024-19016、CNVD-2024-19015）等。
		发布时间	2024-04-23	
		影响产品	Oracle MySQL	
8	Adobe 多款产品存在安全漏洞	**CNVD 编号**	CNVD-2024-15720、CNVD-2024-17889CNVD-2024-17888、CNVD-2024-17892CNVD-2024-17891、CNVD-2024-17890CNVD-2024-19000、CNVD-2024-19002CNVD-2024-19005、CNVD-2024-19008	本月，Adobe 多款产品存在安全漏洞。攻击者可利用该漏洞获取敏感信息，注入精心设计的有效载荷执行任意 Web 脚本或 HTML，在当前用户的上下文中执行任意代码等。本月漏洞包括：Adobe Animate 输入验证错误漏洞（CNVD-2024-19002）、Adobe Animate 缓冲区溢出漏洞（CNVD-2
		其他编号	CVE-2024-20761、CVE-2024-26076 CVE-2024-26046、CVE-2024-26098 CVE-2024-26087、CVE-2024-20778 CVE-2024-20797、CVE-2024-20795	

			CVE-2024-30272、CVE-2024-20758	024-15720、CNVD-2024-19000）、Adobe Experience Manager 信息泄露漏洞（CNVD-2024-17889）、Adobe Experience Manager 跨站脚本漏洞(CNVD-2024-17888、CNVD-2024-17892、CNVD-2024-17891、CNVD-2024-17890）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2024-19005）、Adobe Commerce 输入验证错误漏洞（CNVD-2024-19008）等。
		发布时间	2024-04-15	
		影响产品	Adobe Animate Adobe Experience Manager AEM Cloud Service (CS) Adobe Illustrator Adobe Commerce	

4 月份重要漏洞信息