天融信安全服务

安全通告

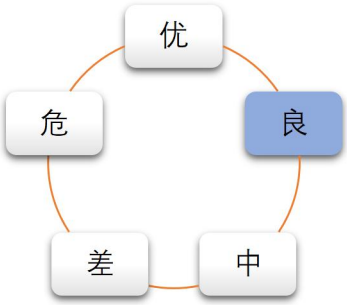
2025 年第 241 期（20250305）

目录

1. 安全态势

1.1. 网络安全基本态势

本期网络安全基本态势评级为“良”：



安全态势较上期环比差异：

↓ 12.2%	• 境内计算机恶意程序传播次数
↓ 15.7%	• 境内被植入后门网站总数
↑ 218.1%	• 境内网站仿冒网页次数
↑ 53.6%	• 新增信息安全漏洞数量

---安全态势数据来源于国家应急互联网应急中心

https://www.cert.org.cn/

1.2. 本期漏洞情况

-----漏洞数据来源 www.cnvd.org.cn

1.2.1. 整体漏洞情况

1.2.2. 重点厂家漏洞分布情况

本期主要针对 Cisco、IBM、Google、Microsoft、Oracle、Adobe、Apple 七个重点厂家新增漏洞数量进行关注，各家新增漏洞情况如下：

厂家名称	Cisco	IBM	Google	Microsoft	Oracle	Adobe	Apple
漏洞数量	0	0	0	0	0	0	0

1.2.3. 重要漏洞信息

1、Adobe 产品安全漏洞

漏洞名称	Adobe InDesign 代码执行漏洞（CNVD-2025-03642）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign <=ID20.0 Adobe InDesign <=ID19.5.1
CVE 编号	CVE-2025-21158
漏洞描述	Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe InDesign 存在代码执行漏洞，攻击者可利用该漏

	洞在当前用户的环境中执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb25-01.html

漏洞名称	Adobe InDesign 越界写入漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign <=ID20.0 Adobe InDesign <=ID19.5.1
CVE 编号	CVE-2025-21157
漏洞描述	Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe InDesign 存在越界写入漏洞，攻击者可利用该漏洞在当前用户的环境中执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb25-01.html

漏洞名称	Adobe Commerce 安全绕过漏洞（CNVD-2025-03635）
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:N)
影响产品	Adobe Adobe Commerce 2.4.8-beta1 Adobe Adobe Commerce <=2.4.7-p3 Adobe Adobe Commerce <=2.4.6-p8

	Adobe Adobe Commerce <=2.4.5-p10 Adobe Adobe Commerce <=2.4.4-p11 Adobe Adobe Commerce B2B <=1.5.0 Adobe Adobe Commerce B2B <=1.4.2-p3 Adobe Adobe Commerce B2B <=1.3.5-p8 Adobe Adobe Commerce B2B <=1.3.4-p10 Adobe Adobe Commerce B2B <=1.3.3-p11 Adobe Magento Open Source 2.4.8-beta1 Adobe Magento Open Source <=2.4.7-p3 Adobe Magento Open Source <=2.4.6-p8 Adobe Magento Open Source <=2.4.5-p10 Adobe Magento Open Source <=2.4.4-p11
CVE 编号	CVE-2025-24411
漏洞描述	Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在安全绕过漏洞，攻击者可利用该漏洞导致安全功能绕过。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/magento/apsb25-08.html

漏洞名称	Adobe InDesign 越界写入漏洞

危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign <=ID20.0 Adobe InDesign <=ID19.5.1
CVE 编号	CVE-2025-21121
漏洞描述	Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe InDesign 存在越界写入漏洞，攻击者可利用该漏洞在当前用户的环境中执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb25-01.html

漏洞名称	Adobe Commerce 安全绕过漏洞（CNVD-2025-03632）
危害级别	中(AV:N/AC:L/Au:S/C:C/I:N/A:N)
影响产品	Adobe Adobe Commerce 2.4.8-beta1 Adobe Adobe Commerce <=2.4.7-p3 Adobe Adobe Commerce <=2.4.6-p8 Adobe Adobe Commerce <=2.4.5-p10 Adobe Adobe Commerce <=2.4.4-p11 Adobe Adobe Commerce B2B <=1.5.0 Adobe Adobe Commerce B2B <=1.4.2-p3 Adobe Adobe Commerce B2B <=1.3.5-p8

	Adobe Adobe Commerce B2B <=1.3.4-p10 Adobe Adobe Commerce B2B <=1.3.3-p11 Adobe Magento Open Source 2.4.8-beta1 Adobe Magento Open Source <=2.4.7-p3 Adobe Magento Open Source <=2.4.6-p8 Adobe Magento Open Source <=2.4.5-p10 Adobe Magento Open Source <=2.4.4-p11
CVE 编号	CVE-2025-24422
漏洞描述	Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在安全绕过漏洞，攻击者可利用该漏洞导致安全功能绕过。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/magento/apsb25-08.html

漏洞名称	Adobe Commerce 安全绕过漏洞（CNVD-2025-03631）
危害级别	中(AV:N/AC:L/Au:S/C:N/I:C/A:N)
影响产品	Adobe Adobe Commerce 2.4.8-beta1 Adobe Adobe Commerce <=2.4.7-p3 Adobe Adobe Commerce <=2.4.6-p8 Adobe Adobe Commerce <=2.4.5-p10

	Adobe Adobe Commerce <=2.4.4-p11 Adobe Adobe Commerce B2B <=1.5.0 Adobe Adobe Commerce B2B <=1.4.2-p3 Adobe Adobe Commerce B2B <=1.3.5-p8 Adobe Adobe Commerce B2B <=1.3.4-p10 Adobe Adobe Commerce B2B <=1.3.3-p11 Adobe Magento Open Source 2.4.8-beta1 Adobe Magento Open Source <=2.4.7-p3 Adobe Magento Open Source <=2.4.6-p8 Adobe Magento Open Source <=2.4.5-p10 Adobe Magento Open Source <=2.4.4-p11
CVE 编号	CVE-2025-24427
漏洞描述	Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在安全绕过漏洞，攻击者可利用该漏洞导致安全功能绕过。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/magento/apsb25-08.html

漏洞名称	Adobe Commerce 安全绕过漏洞（CNVD-2025-03630）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:N/A:N)

影响产品	Adobe Adobe Commerce 2.4.8-beta1 Adobe Adobe Commerce <=2.4.7-p3 Adobe Adobe Commerce <=2.4.6-p8 Adobe Adobe Commerce <=2.4.5-p10 Adobe Adobe Commerce <=2.4.4-p11 Adobe Adobe Commerce B2B <=1.5.0 Adobe Adobe Commerce B2B <=1.4.2-p3 Adobe Adobe Commerce B2B <=1.3.5-p8 Adobe Adobe Commerce B2B <=1.3.4-p10 Adobe Adobe Commerce B2B <=1.3.3-p11 Adobe Magento Open Source 2.4.8-beta1 Adobe Magento Open Source <=2.4.7-p3 Adobe Magento Open Source <=2.4.6-p8 Adobe Magento Open Source <=2.4.5-p10 Adobe Magento Open Source <=2.4.4-p11
CVE 编号	CVE-2025-24429
漏洞描述	Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在安全绕过漏洞，攻击者可利用该漏洞导致安全功能绕过。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/magento/apsb2

	5-08.html

漏洞名称	Adobe Commerce 安全绕过漏洞（CNVD-2025-03626）
危害级别	高(AV:N/AC:L/Au:S/C:C/I:P/A:N)
影响产品	Adobe Adobe Commerce 2.4.8-beta1 Adobe Adobe Commerce <=2.4.7-p3 Adobe Adobe Commerce <=2.4.6-p8 Adobe Adobe Commerce <=2.4.5-p10 Adobe Adobe Commerce <=2.4.4-p11 Adobe Adobe Commerce B2B <=1.5.0 Adobe Adobe Commerce B2B <=1.4.2-p3 Adobe Adobe Commerce B2B <=1.3.5-p8 Adobe Adobe Commerce B2B <=1.3.4-p10 Adobe Adobe Commerce B2B <=1.3.3-p11 Adobe Magento Open Source 2.4.8-beta1 Adobe Magento Open Source <=2.4.7-p3 Adobe Magento Open Source <=2.4.6-p8 Adobe Magento Open Source <=2.4.5-p10 Adobe Magento Open Source <=2.4.4-p11
CVE 编号	CVE-2025-24407
漏洞描述	Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家

	和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在安全绕过漏洞，攻击者可利用此漏洞可能执行未授予权限的操作。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/magento/apsb25-08.html

2、Apache 产品安全漏洞

漏洞名称	Apache Traffic Control SQL 注入漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Apache Traffic Control >=8.0.0，<8.0.2
CVE 编号	CVE-2024-45387
漏洞描述	Apache Traffic Control 是美国阿帕奇（Apache）基金会的一套分布式、可扩展的内容分发解决方案。该产品主要用于构建大规模内容分发网络。Apache Traffic Control 存在 SQL 注入漏洞，该漏洞源于 Traffic Ops 缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/t38nk5n7t8w3pb66z7z4pqfzt4443trr

漏洞名称	Apache OFBiz 输入验证错误漏洞（CNVD-2025-03546）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Apache Apache OFBiz <18.12.17
CVE 编号	CVE-2024-48962
漏洞描述	Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache OFBiz 18.12.17 之前版本存在输入验证错误漏洞，该漏洞源于使用的特殊元素中和不当，攻击者可利用该漏洞导致代码注入和跨站请求伪造(CSRF)漏洞。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/6sddh4pts90cp8ktshqb4xykdp6lb6q6

漏洞名称	Apache Ranger 跨站脚本漏洞（CNVD-2025-03540）
危害级别	中(AV:N/AC:L/Au:M/C:P/I:P/A:N)
影响产品	Apache Apache Ranger 2.4.0
CVE 编号	CVE-2024-45478
漏洞描述	Apache Ranger是美国阿帕奇(Apache)基金会的一套为Hadoop集群实现全面安全措施的架构。该产品针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。Apache Ranger 2.4.0 版本存在跨站脚本漏洞，该漏洞源于 Apache Ranger UI 的

	编辑服务页面对用户提供的数据缺乏有效过滤与转义，攻击者利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger

漏洞名称	Apache Wicket 资源管理错误漏洞
危害级别	中(AV:N/AC:L/Au:S/C:N/I:N/A:C)
影响产品	Apache Wicket 7.0.0
CVE 编号	CVE-2024-53299
漏洞描述	Apache Wicket 是美国阿帕奇（Apache）基金会的一套开源、轻量、基于组件的框架，它提供了一种面向对象的方式来开发基于 Web 的动态 UI 应用程序。Apache Wicket 7.0.0 版本存在资源管理错误漏洞。该漏洞源于应用存在不受控制的资源消耗，攻击者可利用该漏洞导致程序拒绝服务。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/gyp2ht00c62827y0379lxh5dbx3hhho5

漏洞名称	Apache Hadoop 代码注入漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Apache Apache Hadoop

CVE 编号	CVE-2024-51941
漏洞描述	Apache Ambari 是美国阿帕奇 (Apache) 基金会的一个应用软件。提供开发用于配置，管理和监视 Apache Hadoop 集群的软件来简化 Hadoop 管理。 Apache Hadoop 存在代码注入漏洞。该漏洞是由于 Ambari Metrics 和 AMS Alerts 功能中允许经过身份验证的用户注入和执行任意代码，此漏洞发生在处理警报定义时，其中可以将恶意输入注入警报脚本执行路径。攻击者可以利用该漏洞在服务器上执行任意命令。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新:http://www.openwall.com/lists/oss-security/2025/01/21/9

漏洞名称	Apache Linkis 输入验证错误漏洞
危害级别	中(AV:L/AC:L/Au:N/C:P/I:P/A:P)
影响产品	Apache Apache Linkis <1.7.0
CVE 编号	CVE-2024-45627
漏洞描述	Apache Linkis 是美国阿帕奇 (Apache) 基金会的一款中间件产品，可以在上层应用和底层数据引擎之间建立起有效的连接。Apache Linkis 1.7.0 之前版本存在输入验证错误漏洞，该漏洞源于 DataSource Manager 模块中配置恶意的 Mysql JDBC 参数缺乏有效过滤，攻击者可利用该漏洞从 Linkis 服务器读取任意文件。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：

	https://lists.apache.org/thread/0zzx8lldwoqgzq98mg61hojgpvn76xsh

漏洞名称	Apache Cassandra 授权问题漏洞
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Apache Apache Cassandra <4.0.16 Apache Apache Cassandra <4.1.8 Apache Apache Cassandra <5.0.3
CVE 编号	CVE-2025-24860
漏洞描述	Apache Cassandra 是美国阿帕奇（Apache）基金会的一个分布式 Nosql 数据库。Apache Cassandra 存在授权问题漏洞，该漏洞源于包含一个不正确的授权，攻击者可利用该漏洞访问他们在使用 CassandraNetworkAuthorizer 或 CassandraCIDRAuthorizer 时应该无法访问的数据中心或 IP/CIDR 组。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/yjo5on4tf7s1r9qklc4byrz30b8vkm2d

漏洞名称	Apache Ranger 服务端请求伪造漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:N)
影响产品	Apache Apache Ranger 2.4.0
CVE 编号	CVE-2024-45479

漏洞描述	Apache Ranger 是美国阿帕奇（Apache）基金会的一套为 Hadoop 集群实现全面安全措施的架构。该产品针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。Apache Ranger 2.4.0 版本存在服务端请求伪造漏洞，该漏洞源于 Apache Ranger UI 的编辑服务页面未实现足够的验证机制来确认请求的来源，攻击者可利用该漏洞探测服务器内网资源。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger

3、Cisco 产品安全漏洞

漏洞名称	Cisco Meeting Management 权限提升漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Cisco Meeting Management
CVE 编号	CVE-2025-20156
漏洞描述	Cisco Meeting Management 是思科公司用于管理和调度会议的软件。Cisco Meeting Management 存在安全漏洞，该漏洞源于 REST API 用户授权不足，远程攻击者可利用该漏洞通过发送 API 请求到特定端点提升至管理员权限。

漏洞解决方案	目前厂商已发布升级补丁以修复漏洞。补丁获取链接：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc

漏洞名称	Cisco Nexus Dashboard Fabric Controller SQL 注入漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Cisco nexus dashboard fabric controller 12.1
CVE 编号	CVE-2024-20536
漏洞描述	Cisco Nexus Dashboard Fabric Controller 是一款云和数据中心网络管理软件控制器，能够简化数据中心网络的运营和管理。Cisco Nexus Dashboard Fabric Controller 存在 SQL 注入漏洞，远程攻击者可以利用该漏洞提交特殊的 SQL 请求，操作数据库，可获取敏感信息或执行任意代码。
漏洞解决方案	厂商已提供漏洞修复方案，请关注厂商主页更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL

漏洞名称	Cisco Application Policy Infrastructure Controller 访问控制错误漏洞（CNVD-2025-03536）
危害级别	中(AV:N/AC:L/Au:S/C:N/I:P/A:N)
影响产品	Cisco Cisco Application Policy Infrastructure Controller <6.0(6c)

	Cisco Cisco Application Policy Infrastructure Controller <5.3(2c)
CVE 编号	CVE-2024-20279
漏洞描述	Cisco Application Policy Infrastructure Controller（APIC）是美国思科（Cisco）公司的一款自动化的基础架构部署和治理解决方案。Cisco Application Policy Infrastructure Controller 存在访问控制错误漏洞，该漏洞源于使用受限制的安全域来实现多租户时访问控制不当，经过身份验证的远程攻击者可利用该漏洞修改受影响系统上默认系统策略的行为，例如服务质量(QoS)策略。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cousmo-uBpBYGbq

漏洞名称	Cisco Identity Services Engine 代码问题漏洞（CNVD-2025-03531）
危害级别	高(AV:N/AC:L/Au:S/C:P/I:C/A:C)
影响产品	Cisco Identity Services Engine
CVE 编号	CVE-2025-20124
漏洞描述	Cisco Identity Services Engine 是美国思科(Cisco)公司的一款环境感知平台。Cisco Identity Services Engine API 存在代码问题漏洞，远程攻击者可利用该漏洞提交特殊的请求，可以高权限执行

	任意命令。
漏洞解决方案	厂商已提供漏洞修复方案，请关注厂商主页更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF

漏洞名称	Cisco AsyncOS 输入验证错误漏洞（CNVD-2025-03529）
危害级别	高(AV:N/AC:L/Au:M/C:C/I:C/A:N)
影响产品	Cisco Asyncos null
CVE 编号	CVE-2025-20184
漏洞描述	Cisco AsyncOS 是美国思科（Cisco）公司的一款应用于思科设备的操作系统。Cisco AsyncOS 存在输入验证错误漏洞，该漏洞源于 XML 配置文件验证不足，经过身份验证的远程攻击者可利用该漏洞上传特制文件并以 root 权限执行命令。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-multi-yKUJhS34

漏洞名称	Cisco Identity Services Engine 授权绕过漏洞（CNVD-2025-03530）
危害级别	高(AV:N/AC:L/Au:S/C:P/I:P/A:C)
影响产品	Cisco Identity Services Engine
CVE 编号	CVE-2025-20125

漏洞描述	Cisco Identity Services Engine 是美国思科(Cisco)公司的一款环境感知平台。Cisco Identity Services Engine API 存在授权绕过漏洞，远程攻击者可利用该漏洞提交特殊的请求，可获得敏感信息，修改系统配置，重启设备。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF

漏洞名称	Cisco BroadWorks 拒绝服务漏洞
危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	Cisco Cisco BroadWorks
CVE 编号	CVE-2025-20165
漏洞描述	Cisco BroadWorks 是美国思科（Cisco）公司的一个运营商级统一通信软件平台。用于在任何类型的有线或无线网络架构上部署来自公共网络平台的云呼叫。Cisco BroadWorks 存在拒绝服务漏洞，该漏洞源于对某些 SIP 请求的内存处理不当，远程攻击者可利用该漏洞通过发送大量 SIP 请求使处理停止，造成服务拒绝攻击。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-sip-dos-mSySbrmt

漏洞名称	Cisco Expressway Series 跨站脚本漏洞

危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Cisco Cisco Expressway Series <15.2.2
CVE 编号	CVE-2025-20179
漏洞描述	Cisco Expressway Series 是美国思科（Cisco）公司的一款用于防火墙外访问设备的软件。该软件为防火墙外的用户提供了简单、高度安全的访问功能，帮助远程办公人员在他们选择的设备上更有效地工作。Cisco Expressway Series 存在跨站脚本漏洞，该漏洞源于用户输入验证不当，未经身份验证的远程攻击者可利用该漏洞通过特制链接执行任意脚本代码或访问敏感信息。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-xss-uexUZrEW

4、Google 产品安全漏洞

漏洞名称	Google Android 信息泄露漏洞（CNVD-2025-03652）
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Google Android 8.0Google Android 8.1
CVE 编号	CVE-2017-13321
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为

	基础的开源操作系统。Google Android 存在信息泄露漏洞，该漏洞源于 SensorService.cpp 文件中 SensorService::isDataInjectionEnabled 方法缺少边界检查，攻击者可利用该漏洞获取敏感信息。
漏洞解决方案	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://source.android.com/docs/security/bulletin/pixel/2018-05-01

漏洞名称	Google Chrome 代码执行漏洞（CNVD-2025-03651）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <133.0.6943.98
CVE 编号	CVE-2025-0998
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 存在代码执行漏洞，该漏洞是由 V8 中的越界内存访问引起的。攻击者可利用该漏洞在系统上执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_12.html

漏洞名称	Google Chrome 代码执行漏洞（CNVD-2025-03650）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <133.0.6943.98

CVE 编号	CVE-2025-0995
漏洞描述	Google Chrome 是美国谷歌(Google)公司的一款 Web 浏览器。Google Chrome 存在代码执行漏洞，攻击者可利用该漏洞在系统上执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_12.html

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-03647）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14
CVE 编号	CVE-2024-34730
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在权限提升漏洞，该漏洞是由多个位置的逻辑错误引起的。攻击者可利用该漏洞导致本地特权升级。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2025-01-01

漏洞名称	Google Chrome 代码执行漏洞（CNVD-2025-03646）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <133.0.6943.98
CVE 编号	CVE-2025-0997
漏洞描述	Google Chrome 是美国谷歌(Google)公司的一款 Web 浏览器。Google Chrome 存在代码执行漏洞，该漏洞是由于在导航中免费使用造成的。攻击者可利用此漏洞在系统上执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_12.html

漏洞名称	Google Android shouldSkipForInitialSUW 函数授权问题漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14 Google Android <15
CVE 编号	CVE-2024-40677
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在授权问题漏洞，该漏

	洞源于 AdvancedPowerUsageDetail.java 的 shouldSkipForInitialSUW 函数中缺少权限检查，攻击者可利用该漏洞导致绕过出厂重置保护，从而导致本地权限提升。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2024-10-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-03644）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14 Google Android <15
CVE 编号	CVE-2024-43095
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在权限提升漏洞，该漏洞是由于代码中的逻辑错误，攻击者可利用该漏洞导致本地特权升级。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2025-01-01

漏洞名称	Google Android 代码执行漏洞（CNVD-2025-03643）

危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14 Google Android <15
CVE 编号	CVE-2024-43096
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在代码执行漏洞，该漏洞是由系统组件中的缺陷引起的。攻击者可利用该漏洞在系统上执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2025-01-01

5、D-Link DIR-816A2 form2WlanBasicSetup.cgi 组件访问控制错误漏洞

漏洞名称	D-Link DIR-816A2 form2WlanBasicSetup.cgi 组件访问控制错误漏洞
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	D-Link DIR-816A2 FWv1.10CNB05_R1B011D88210

CVE 编号	CVE-2024-57676
漏洞描述	D-Link DIR-816A2 是中国友讯（D-Link）公司的一款路由器。D-Link DIR-816A2 存在访问控制错误漏洞，该漏洞源于 form2WlanBasicSetup.cgi 组件的访问控制不当，未认证攻击者可利用此漏洞通过特制 POST 请求设置 2.4G 和 5G 无线服务。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://www.dlink.com/en/security-bulletin/

1.2.4. 高关注度漏洞预警信息

1.2.4.1. 境外厂商产品漏洞

漏洞名称	Adobe InDesign 越界写入漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign <=ID20.0 Adobe InDesign <=ID19.5.1
CVE 编号	CVE-2025-21157
漏洞描述	Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe InDesign 存在越界写入漏洞，攻击者可利用该漏洞在当前用户的环境中执行任意代码。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：

	https://helpx.adobe.com/security/products/indesign/apsb25-01.html

漏洞名称	Siemens Teamcenter 重定向漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Siemens Teamcenter
CVE 编号	CVE-2025-23363
漏洞描述	Teamcenter 软件是一个适应性强的现代化产品生命周期管理（PLM） 系统，它通过数字主线跨越功能孤岛将人员和流程连接起来，以实现创新。Siemens Teamcenter SSO 登录服务存在重定向漏洞，攻击者可利用漏洞将合法用户重定向到攻击者选择的 URL，以窃取有效的会话数据。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：http://www.siemens.com/

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-03647）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14
CVE 编号	CVE-2024-34730

漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在权限提升漏洞，该漏洞是由多个位置的逻辑错误引起的。攻击者可利用该漏洞导致本地特权升级。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2025-01-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-03644）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <12 Google Android <12L Google Android <13 Google Android <14 Google Android <15
CVE 编号	CVE-2024-43095
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在权限提升漏洞，该漏洞是由于代码中的逻辑错误，攻击者可利用该漏洞导致本地特权升级。
漏洞解决方案	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2025-01-01

漏洞名称	Google Android 信息泄露漏洞（CNVD-2025-03652）
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Google Android 8.0 Google Android 8.1
CVE 编号	CVE-2017-13321
漏洞描述	Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Android 存在信息泄露漏洞，该漏洞源于 SensorService.cpp 文件中 SensorService::isDataInjectionEnabled 方法缺少边界检查，攻击者可利用该漏洞获取敏感信息。
漏洞解决方案	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://source.android.com/docs/security/bulletin/pixel/2018-05-01

1.2.4.2. 境内厂商产品漏洞

漏洞名称	用友网络科技股份有限公司 U8 Cloud 存在 SQL 注入漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	用友网络科技股份有限公司 U8 Cloud
CVE 编号	U8 Cloud 是用友推出的一款新一代云 ERP（企业资源计划）解决方案，主要面向成长型和创新型企业，旨在提供全面的企业级云

	ERP 整体解决方案。
漏洞描述	U8 Cloud 是用友推出的一款新一代云 ERP（企业资源计划）解决方案，主要面向成长型和创新型企业，旨在提供全面的企业级云 ERP 整体解决方案。用友网络科技股份有限公司 U8 Cloud 存在 SQL 注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。
漏洞解决方案	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://security.yonyou.com/#/noticeInfo?id=675

漏洞名称	湖南众合百易信息技术有限公司资管云存在 SQL 注入漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	湖南众合百易信息技术有限公司 资管云
CVE 编号	无
漏洞描述	湖南众合百易信息技术有限公司（简称：百易云）成立于 2017 年是一家专注于不动产领域数字化研发及服务的国家高新技术企业。湖南众合百易信息技术有限公司资管云存在 SQL 注入漏洞，攻击者可利用该漏洞获取数据库敏感信息。
漏洞解决方案	厂商已发布补丁修复漏洞，请广大用户及时下载更新：https://www.baiyishequ.com

漏洞名称	Tenda i12 formwrlSSIDset 缓冲区溢出漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Tenda i12 V1.0.0.10(3805)

CVE 编号	CVE-2025-25676
漏洞描述	Tenda i12 是一款企业商用大功率 AP 无线接入点。Tenda i12 formwrlSSIDset 处理 list 参数存在缓冲区溢出漏洞，远程攻击者可利用该漏洞提交特殊的请求，可使应用程序崩溃，造成拒绝服务攻击。
漏洞解决方案	厂商尚未发布漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/material/show/102572

漏洞名称	Tenda i12 formSetCfm 缓冲区溢出漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Tenda i12 V1.0.0.10(3805)
CVE 编号	CVE-2025-25678
漏洞描述	Tenda i12 是一款企业商用大功率 AP 无线接入点。Tenda i12 formSetCfm 处理 funcpara1 参数存在缓冲区溢出漏洞，远程攻击者可利用该漏洞提交特殊的请求，可使应用程序崩溃，造成拒绝服务攻击。
漏洞解决方案	厂商尚未发布漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/material/show/102572

漏洞名称	D-Link DIR-816A2 form2WlanBasicSetup.cgi 组件访问控制错误漏洞
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)

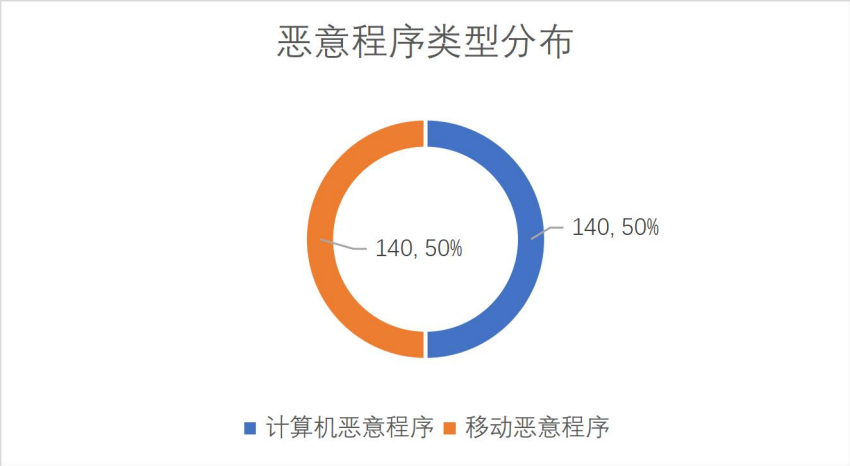
影响产品	D-Link DIR-816A2 FWv1.10CNB05_R1B011D88210
CVE 编号	CVE-2024-57676
漏洞描述	D-Link DIR-816A2 是中国友讯（D-Link）公司的一款路由器。D-Link DIR-816A2 存在访问控制错误漏洞，该漏洞源于 form2WlanBasicSetup.cgi 组件的访问控制不当，未认证攻击者可利用此漏洞通过特制 POST 请求设置 2.4G 和 5G 无线服务。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://www.dlink.com/en/security-bulletin/

1.3. 本期威胁情报

1.3.1. 病毒程序跟踪情况

本期总计新发现病毒程序 280 个，其中计算机病毒程序 140 个，移动病毒程序 140 个。

恶意程序类型分布图如下：



计算机恶意程序抽取 20 条记录如下：

病毒名称	操作系统	发布时间
PUP.Win32.LoadMoney.XV	Win32	2025-03-03
PUP.Win32.LoadMoney.XV	Win32	2025-03-03
Trojan.Win32.ATRAPS.Gen5	Win32	2025-03-03
Trojan.Win32.ATRAPS.Gen5	Win32	2025-03-03
Worm.Win32.AutoRun.QN	Win32	2025-03-03
Worm.Win32.AutoRun.QN	Win32	2025-03-03
Trojan.Win32.InstallMonst.QA	Win32	2025-03-03
Trojan.Win32.InstallMonst.QA	Win32	2025-03-03
Trojan.Win32.Ponmocup.AA	Win32	2025-03-03
Trojan.Win32.Ponmocup.AA	Win32	2025-03-03

Trojan.Win32.Vemply.gen	Win32	2025-03-03
Trojan.Win32.Vemply.gen	Win32	2025-03-03
Trojan.Win32.Adload.AQ	Win32	2025-03-03
Trojan.Win32.Adload.AQ	Win32	2025-03-03
PUP.Win32.Crossrider.DL	Win32	2025-03-03
PUP.Win32.Crossrider.DL	Win32	2025-03-03
Exploit.HTML.ExpKit.Gen2	HTML	2025-03-03
Exploit.HTML.ExpKit.Gen2	HTML	2025-03-03
Adware.Win32.MultiPlug.m	Win32	2025-03-03
Adware.Win32.MultiPlug.m	Win32	2025-03-03

移动恶意程序抽取 20 条记录如下：

病毒名称	操作系统	发布时间
a.remote.FakeInst.j	Android	2025-03-03
a.remote.FakeInst.j	Android	2025-03-03
a.rogue.Youmi.b	Android	2025-03-03
a.rogue.Youmi.b	Android	2025-03-03
a.remote.SAgnt.ac	Android	2025-03-03
a.remote.SAgnt.ac	Android	2025-03-03
a.remote.Obfus.oa	Android	2025-03-03

a.remote.Obfus.oa	Android	2025-03-03
a.privacy.Secapk.e	Android	2025-03-03
a.privacy.Secapk.e	Android	2025-03-03
a.remote.Obfus.oa	Android	2025-03-03
a.remote.Obfus.oa	Android	2025-03-03
a.rogue.Kirko.a	Android	2025-03-03
a.rogue.Kirko.a	Android	2025-03-03
a.privacy.Robtes.dm	Android	2025-03-03
a.privacy.Robtes.dm	Android	2025-03-03
a.rogue.Domob.a	Android	2025-03-03
a.rogue.Domob.a	Android	2025-03-03
a.remote.DroidKungFu.r	Android	2025-03-03
a.remote.DroidKungFu.r	Android	2025-03-03

2. 安全资讯

2.1. 新型后门程序利用 polyglot 文件传播

Proofpoint 报告指出，威胁行为者已将该手法用于针对阿联酋关键基础设施企业的攻击，并警告各地 CISO 需警惕其扩散。某威胁行为者正在使用 polyglot 文件隐藏新型后门程序的安装，这是针对阿联酋企业，特别是航空、卫星通信和交通行业的鱼叉式钓鱼攻击的一部分。

Proofpoint 的研究人员在 PwC 威胁情报团队的协助下发现了这一后门程序，并将其命名为 Sosano。

该攻击目前可能仅限于阿联酋，但各地的 CISO 都应提高警惕，因为这种手法和后门程序可能扩散到其他地区。

Proofpoint 表示，威胁行为者使用 polyglot 文件的行为“相对不常见于以间谍活动为动机的攻击者”。polyglot 文件是通过精心构建数据，使不同解析器对同一文件产生不同解释，通常利用特定格式的缺陷或重叠头文件来实现。

恶意软件活动中使用多语文件的一个例子是 Emmenhtal 加载器，Proofpoint 称其经常出现在网络犯罪攻击链中，用于传递信息窃取程序或远程访问木马（RAT）。

Beauceron Security 公司的首席执行官 David Shipley 表示：“这份报告显示，攻击者在目标选择和社交工程引诱方面具有高度复杂性，同时在使用多语文件方面也表现出同等的技术水准。”他强调：“这说明攻击者与防御者之间的博弈仅受限于攻击者的创造力和时间投入，同时也突显了技术控制和积极安全文化的持久重要性，这种文化能激励人们发现、阻止并报告威胁。”

2.2. VMware ESX 曝 3 个 0Day 漏洞，已被黑客利用

Broadcom 发布了安全更新，以修复 VMware ESX 产品中的三个 0Day 漏洞。这些漏洞分别被标识为 CVE-2025-22224、CVE-2025-22225 和 CVE-2025-22226，影响了多个 VMware ESX 产品，包括 VMware ESXi、vSphere、Workstation、Fusion、Cloud Foundation 和 Telco Cloud Platform。

这些漏洞由微软威胁情报中心的研究人员发现。攻击者如果拥有管理员或 root 权限，可以链式利用这些漏洞，从虚拟机中逃脱沙盒限制。

VMware 确认，已有信息表明这些漏洞在野外被利用。2025 年 3 月 4 日，Broadcom 发布了关键 VMware 安全公告（VMSA-2025-0004），解决了 VMware ESX 中的安全漏洞，这些漏洞使得威胁者可以通过运行的虚拟机访问管理程序。

Broadcom 表示，攻击者已经利用这些漏洞进行了虚拟机逃逸(VM Escape)。具体来说，攻击者在已经攻破虚拟机客户操作系统并获得特权访问（管理员或 root 权限）后，可以进一步进入管理程序本身。

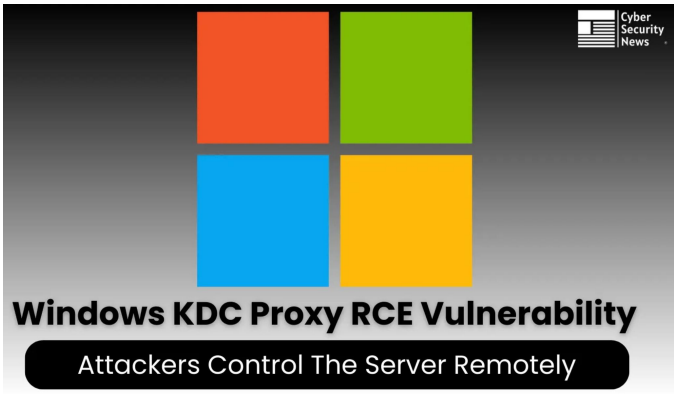
目前，该公司尚未披露有关攻击的具体细节或幕后威胁者的信息。

2.3. Windows KDC 曝代理 RCE 漏洞：攻击者可远程控制服务器

安全研究人员近日在微软的 Windows 密钥分发中心（KDC）代理中发现了一个严重的远程代码执行漏洞（CVE-2024-43639），攻击者可能利用该漏洞完全控制受影响的服务器。该漏洞源于 KDC 代理服务中缺乏对 Kerberos 响应长度的检查，导致整数溢出，从而使得未经身份验证的远程攻击者能够以目标服务的权限执行任意代码，可能导致系统完全沦陷。

攻击者通过控制一个服务器并返回精心构造的 Kerberos 响应，利用 KpsSocketRecvDataIoCompletion()函数未对响应长度进行验证的缺陷触发整数溢出。漏洞在 ASN.1 编码过程中导致内存分配或重新分配失败，从而引发内存损坏。攻击者甚至可以绕过现有的验证机制，直接进入易受攻击的代码路径。

微软已在 2024 年 11 月的安全更新中修复该漏洞，对 KDC 代理服务器服务中的响应长度添加了验证检查。建议运行 KDC 代理的机构立即应用该补丁。若无法立即修补，可考虑暂时禁用 KDC 代理服务，尽管这可能会影响企业网络外部用户的远程认证能力。此外，安全团队还应监控 TCP 端口 88 的流量，检测潜在的可疑活动。



2.4. 最新黑产技术曝光，只需 19 分钟即可劫持 AI 大模型

安全公司 Entro Labs 最近在 GitHub、Pastebin 和 Reddit 上发布了功能性 AWS 密钥，以研究攻击者的行为。

他们的研究揭示了一种系统化的四阶段攻击模式：

凭证收集：自动化的机器人使用 Python 脚本扫描公共代码库和论坛，以检测有效凭证，其中 44%的非人类身份是通过代码库和协作平台泄露的。

快速验证：攻击者在凭证暴露后的 9-17 分钟内执行初始 API 调用（如 GetCostAndUsage）以评估账户价值，并避免使用可预测的调用（如 GetCallerIdentity）以逃避检测。

模型枚举：入侵者通过 AWS Bedrock 执行 GetFoundationModelAvailability 请求，以列出可访问的 LLM——包括 Anthropic 的 Claude 和 Amazon Titan——并映射可用的攻击面。

利用：攻击者对受损端点进行自动化的 InvokeModel 尝试，研究人员在实验密钥中观察到每小时超过 1200 次未经授权的推理尝试。

随着攻击者在 20 分钟内即可利用泄露的密钥，实时密钥扫描和自动轮换不再是一种可选的保护措施，而是 LLM 时代的关键生存机制。

2.5. 剖析 Black Basta 勒索软件入侵策略：泄露日志揭示的攻击手法

补丁管理公司Qualys的研究人员在对泄露日志的分析中写道："Black Basta使用的主要攻击向量包括扫描暴露的 RDP（远程桌面协议）和 VPN 服务——通常依赖默认 VPN 凭证或暴力破解窃取的凭证来获得初始访问——以及在系统未打补丁时利用公开已知的 CVE。"

同时，网络威胁情报公司 KELA 观察到泄露日志中存在的 3000 个独特凭证与之前信息窃取恶意软件的数据转储之间的相关性，表明其与其他收集并出售此类数据的威胁组织有关联。

Qualys 的研究人员写道："KELA 看到这些攻击者利用漏洞和网络钓鱼/垃圾邮件活动获取凭证，以及使用被攻陷的电子邮件凭证，然后在电子邮件对话中寻找远程访问凭证。然后，这些凭证要么作为初始访问向量，要么用于横向移动阶段。"

最后，该组织经常依赖面向互联网设备的公开已知漏洞，尤其是那些已有概念验证利用的漏洞。根据漏洞情报公司 VulnCheck 的研究人员分析，泄露的 Black Basta 日志包含了 62 个独特的 CVE。

日志中提到的一些漏洞虽然古老但仍然广泛存在，例如微软 Office 远程模板功能中的 CVE-2022-30190 远程代码执行漏洞，也称为 Follina 漏洞，已通过恶意 Word 附件被广泛利用。其他知名漏洞包括 Log4Shell（CVE-2021-44228）、Spring4Shell（CVE-2022-22965）和 ProxyNotShell（CVE-2022-41028，CVE-2022-41040）。

2.6. 黑客利用 Safe 实施供应链攻击

美国联邦调查局（FBI）日前正式将 Bybit 遭受创纪录的 15 亿美元加密货币被窃事件与朝鲜黑客组织 Lazarus 联系起来。与此同时，Bybit 的首席执行官 Ben Zhou 宣布要对 Lazarus 全面”开战“

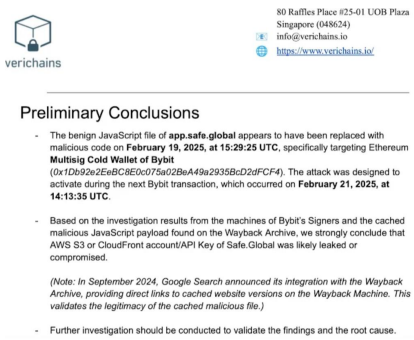
FBI 表示，朝鲜应对此次加密货币交易所的虚拟资产盗窃事件负责。该事件被归咎于 FBI 追踪的一个特定集群 TraderTraitor，该集群也被称为 Jade Sleet、Slow Pisces 和 UNC4899。

FBI 称：“TraderTraitor 的行为迅速，已将部分被盗资产转换为比特币和其他虚拟资产，并分散在多个区块链上的数千个地址中。预计这些资产将被进一步洗钱，并最终转换为法定货币。”

值得一提的是，TraderTraitor 集群此前曾被日本和美国当局指控参与 2024 年 5 月从加密货币公司 DMM Bitcoin 窃取价值 3.08 亿美元加密货币的事件。

总部位于迪拜的 Bybit 还分享了由 Sygnia 和 Verichains 进行的两项调查的结论，将此次攻击与 Lazarus 集团联系起来。

Sygnia 表示：“对三个签名者主机的取证调查表明，攻击的根本原因是从 Safe{Wallet} 基础设施中产生的恶意代码。



verichains

80 Raffles Place #25-01 UOB Plaza
Singapore (048624)
info@verichains.io
https://www.verichains.io/

Preliminary Conclusions

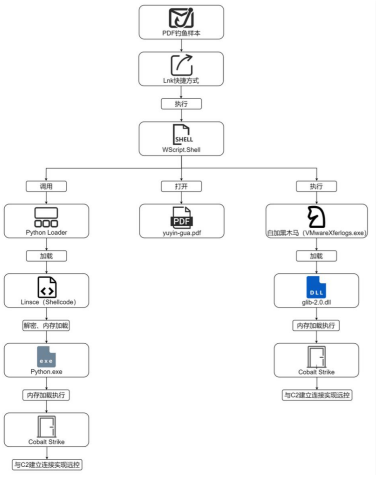
- The benign JavaScript file of **app.safe.global** appears to have been replaced with malicious code on **February 19, 2025, at 15:29:25 UTC**, specifically targeting Ethereum **Multisig Cold Wallet of Bybit** (*0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4*). The attack was designed to activate during the next Bybit transaction, which occurred on **February 21, 2025, at 14:13:35 UTC**.
- Based on the investigation results from the machines of Bybit's Signers and the cached malicious JavaScript payload found on the Wayback Archive, we strongly conclude that AWS S3 or CloudFront account/API Key of Safe.Global was likely leaked or compromised.

  (Note: In September 2024, Google Search announced its integration with the Wayback Archive, providing direct links to cached website versions on the Wayback Machine. This validates the legitimacy of the cached malicious file.)
- Further investigation should be conducted to validate the findings and the root cause.

2.7. 钓鱼攻击通过 PDF 文档暗投后门病毒

钓鱼攻击是一种高度隐蔽且极具欺骗性的网络威胁，攻击者通过伪装成银行、保险公司、税务机构或其他可信机构的官方文件，诱导受害者点击下载恶意文件。而在生活和工作中，电子文档作为常用工具，可能也不会让我们“心生防备”。因此电子文档可以成为网络钓鱼攻击的常用媒介，攻击者可以通过表象的“电子文档”来掩盖快捷方式和隐藏文件夹实际的恶意行为，并且电子文档的复杂性和灵活性也导致恶意代码潜藏很深，难以被普通用户察觉，令个人和企业面临财务损失和数据泄露的风险。

近期，威胁情报中心检测到恶意钓鱼 PDF 样本攻击量增多，且个别样本通过伪装成快捷方式和隐藏文件夹的方式进行传播。经工程师分析，该木马程序采用双重攻击机制：一方面通过 VBS 脚本执行 Python 加载器，另一方面利用“白加黑”技术执行恶意文件，最终部署 Cobalt Strike 远控后门。建议日常可以通过关注可疑的发件人地址、不寻常的链接或过于紧急的要求来规避此风险。同时技术防护手段也不可或缺，如安装可靠的安全软件，对邮件和文件进行实时扫描和检测，监控异常的网络行为。



2.8. 谷歌官方应用 SafetyCore 暗中扫描用户手机中的照片

与常规应用安装不同，SafetyCore 没有图标，隐藏在系统进程中，并占用了约 2GB 的存储空间。这一细节在一篇广泛传播的 X（原 Twitter）帖子中被曝光，帖子指责谷歌暗中开启了照片库扫描功能。用户只有在进入“设置 > 应用 > 显示系统进程”时，才能发现该应用作为后台服务存在，并拥有互联网访问、存储和设备传感器等权限。

尽管谷歌澄清 SafetyCore 仅为“设备端基础设施”，用于支持如 Google Messages 等应用的敏感内容警告功能（如模糊处理潜在露骨图片并在发送或接收前提醒用户），但其隐蔽的安装方式仍引发了对用户知情权和企业责任的质疑。

SafetyCore 使用机器学习（ML）模型在本地对内容进行分类，保持端到端加密，避免云端数据传输。其架构与客户端扫描（CSS）技术一致，CSS 是一种在本地而非远程服务器上处理数据的隐私保护技术。然而，CSS 因其可能被滥用的风险而备受争议。安全专家警告，此类系统可能超出其最初设计的范围，使政府或企业能够监控与之无关的内容。

谷歌坚称 SafetyCore 仅限于“选择加入”的功能，但其静默部署削弱了用户的信任，因为用户并未被告知该服务的安装或功能。值得注意的是，SafetyCore 独立于谷歌的现有恶意软件扫描工具 Google Play Protect，专注于内容审核。此次针对 SafetyCore 的抵制与苹果 2022 年因 iMessage 中的通信安全功能引发的争议类似。虽然苹果因默认启用照片扫描功能而受到批评，但它提供了清晰的文档和用户控制选项，这与谷歌的隐晦部署形成鲜明对比。

2.9. 黑客团伙 Anonymous Sudan 被 FBI 重创，组织者被判终身监禁

Anonymous Sudan 掌握着庞大的分布式拒绝服务（DDoS）僵尸网络，在短短一年内实施了创纪录的 35000 次 DDoS 攻击，其中包括 2023 年 6 月针对微软服务的攻击。Microsoft 365 系列服务因为被攻击经常发现访问中断，这严重影响到部分用户的正常办公。

美国司法部（DoJ）表示，这些攻击由 Anonymous Sudan 的“强大 DDoS 工具”促成，专门针对美国及全球的关键基础设施、企业网络和政府机构。因此，22 岁的 Ahmed Salah Yousif Omer （艾哈迈德·萨拉赫 ）和 27 岁的 Alaa Salah Yusuuf Omer （阿拉·萨拉赫 ）被指控的一项罪名是共谋破坏受保护计算机。此外，艾哈迈德还被指控其他三项“破坏受保护的计算机”的罪名。

如果所有罪名成立，艾哈迈德·萨拉赫将面临法定最高刑期终身监禁，而阿拉·萨拉赫将面临最高五年的联邦监狱刑期。

据悉，该 DDoS 工具已于 2024 年 3 月被禁用，同月两人从某个未知国家被捕。美国检察官马丁·埃斯特拉达表示，“匿名苏丹试图通过对全球政府和商业实施数万次网络攻击来最大化混乱和破坏，这个组织的攻击冷酷无情，甚至多次攻击为患者提供紧急和急症护理的医院。”

美国司法部表示，这些执法行动是作为 Operation PowerOFF 的一部分采取的。

2.10. 新的 macOS 漏洞允许攻击者绕过安全控制

据 Cyber Security News 消息，微软威胁情报发现，macOS 出现了一个名为“HM Surf”的新漏洞，能允许攻击者绕过操作系统的透明、同意和控制（TCC）技术，在未经授权的情况下访问用户受保护的数据。

该漏洞被追踪为 CVE-2024-44133，能够被利用收集敏感信息（例如浏览历史记录），并在未经授权的情况下访问设备的摄像头、麦克风和位置。

HM Surf 能够更改当前用户的主目录，修改用户真实主目录下的敏感文件，以及运行 Safari 打开一个网页，该网页拍摄相机快照并跟踪设备位置。

攻击者可以执行一些隐秘的操作，例如私下托管快照、保存整个摄像头数据流、录制和串流麦克风音频，以及在小窗口中启动 Safari 以避免引起注意。

微软通过 Microsoft Security Vulnerability Research （MSVR） 的协调漏洞披露 （CVD） 与 苹果分享了这一漏洞发现。目前，只有 Safari 使用 TCC 提供的新保护，微软正在与其他主要浏览器供应商合作，以调查强化本地配置文件的好处。