天融信安全服务

安全通告

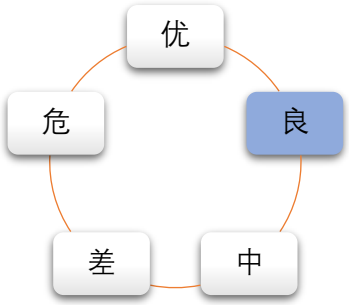
2025 年 6 月 4 日

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：

- 境内计算机恶意程序传播次数 7.9%
- 境内被植入后门网站总数 73.6%
- 境内网站仿冒网页次数 8.6%
- 新增信息安全漏洞数量 13.2%

---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	8	15	0	12	1

1.2.3. 重要漏洞信息

1、Adobe 产品安全漏洞

漏洞名称	Adobe Connect 跨站脚本漏洞（CNVD-2025-10676）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Connect <=12.8
CVE 编号	CVE-2025-30316
漏洞描述	Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Connect 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript。

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/connect/apsb25-36.html

漏洞名称	Adobe Connect 跨站脚本漏洞（CNVD-2025-10674）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Adobe Adobe Connect <=12.8
CVE 编号	CVE-2025-30315
漏洞描述	Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Connect 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript。
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/connect/apsb25-36.html

漏洞名称	Adobe Connect 跨站脚本漏洞（CNVD-2025-10675）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Adobe Adobe Connect <=12.8
CVE 编号	CVE-2025-30314
漏洞描述	Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Connect 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript。

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/connect/apsb25-36.html

漏洞名称	Adobe ColdFusion 路径遍历漏洞（CNVD-2025-10673）
危害级别	中(AV:N/AC:L/Au:M/C:C/I:N/A:N)
影响产品	Adobe ColdFusion 2025 Update 1Adobe ColdFusion 2023 <=Update 13Adobe ColdFusion 2021 <=Update 19
CVE 编号	CVE-2025-43566
漏洞描述	Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。Adobe ColdFusion 存在路径遍历漏洞，该漏洞源于路径名限制不当，攻击者可利用该漏洞读取任意文件系统。
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/coldfusion/apsb25-52.html

漏洞名称	Adobe Bridge 输入验证错误漏洞（CNVD-2025-10671）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Adobe Bridge <=15.0.3Adobe Adobe Bridge <=14.1.6
CVE 编号	CVE-2025-43547
漏洞描述	Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。

	Adobe Bridge 存在输入验证错误漏洞，该漏洞源于整数溢出，攻击者可利用该漏洞执行任意代码。
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/bridge/apsb25-44.html

漏洞名称	Adobe Bridge 缓冲区溢出漏洞（CNVD-2025-10670）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Adobe Bridge <=15.0.3Adobe Adobe Bridge <=14.1.6
CVE 编号	CVE-2025-43545
漏洞描述	Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe Bridge 存在缓冲区溢出漏洞，该漏洞源于未初始化指针访问，攻击者可利用该漏洞执行任意代码。
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/bridge/apsb25-44.html

漏洞名称	Adobe Animate 越界写入漏洞（CNVD-2025-10667）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Adobe Animate 2023 <=23.0.11Adobe Adobe Animate 2024 <=24.0.8
CVE 编号	CVE-2025-30328

漏洞描述	Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Animate 存在越界写入漏洞，攻击者可利用该漏洞执行任意代码。
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/animate/apsb25-42.html

漏洞名称	Adobe Animate 输入验证错误漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Adobe Animate 2023 <=23.0.11Adobe Adobe Animate 2024 <=24.0.8
CVE 编号	CVE-2025-43556
漏洞描述	Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Animate 存在输入验证错误漏洞，该漏洞源于整数溢出，攻击者可利用该漏洞执行任意代码。
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/animate/apsb25-42.html

2、Microsoft 产品安全漏洞

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10663）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-24057
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-24057

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10659）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Office Online Server Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office

	LTSC for Mac 2024 Microsoft SharePoint Server Subscription Edition Language Pack
CVE 编号	CVE-2025-27746
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27746

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10660）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-27745
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27745

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10657）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-27749
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27749

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10658）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)

影响产品	Microsoft Office 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-27748
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27748

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10614
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Access 2016 Microsoft Excel 2016 Microsoft Office Online Server Microsoft Office 2019 Microsoft SharePoint Server 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024

CVE 编号	CVE-2025-26642
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-26642

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10613）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft 365 Apps for Enterprise Microsoft Office 2016 Microsoft Office 2019 Microsoft Office LTSC 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC for Mac 2024 Microsoft Office for Android
CVE 编号	CVE-2025-30377
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-30377

漏洞名称	Microsoft Office 代码执行漏洞（CNVD-2025-10612）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Office for Android Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-30386
漏洞描述	Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Office 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-30386

3、ZTE 产品安全漏洞

漏洞名称	ZTE GoldenDB 未授权访问漏洞（CNVD-2025-10902）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03，<=6.1.03.05
CVE 编号	CVE-2025-26705
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在未授权访问漏洞，该漏洞源于权限管理不当，攻击者可利用该漏洞在未经授权的情况下通过接口获取信息。
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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/577084989971263576

漏洞名称	ZTE GoldenDB 未授权访问漏洞
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03，<=6.1.03.05
CVE 编号	CVE-2025-26707
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在未授权访问漏洞，该漏洞源于权限管理不

	当，攻击者可利用该漏洞在未经授权的情况下通过接口获取信息。
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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/6999218053484646470

漏洞名称	ZTE GoldenDB 权限提升漏洞
危害级别	中(AV:N/AC:L/Au:S/C:N/I:P/A:P)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03，<=6.1.03.07
CVE 编号	CVE-2025-26706
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在权限提升漏洞，该漏洞源于权限管理不当，攻击者可利用该漏洞提升权限。
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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/6999218053484646486

漏洞名称	ZTE GoldenDB 访问控制错误漏洞
危害级别	中(AV:N/AC:L/Au:S/C:N/I:P/A:P)
影响产品	ZTE ZXCLOUD GoldenDB 7.2.01.01ZTE ZXCLOUD GoldenDB Lite7.2.01.01ZTE ZXCLOUD GoldenDB 6.1.03.09ZTE ZXCLOUD GoldenDB 6.1.03.10

CVE 编号	CVE-2025-46576
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在访问控制错误漏洞，该漏洞源于权限管理和访问控制不当，攻击者可利用该漏洞操纵请求以绕过权限限制并删除内容。
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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/10364676150916014 64

漏洞名称	ZTE GoldenDB 信息泄露漏洞
危害级别	中(AV:N/AC:L/Au:M/C:C/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB 7.2.01.01ZTE ZXCLOUD GoldenDB Lite7.2.01.01ZTE ZXCLOUD GoldenDB 6.1.03.09ZTE ZXCLOUD GoldenDB 6.1.03.10
CVE 编号	CVE-2025-46575
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在信息泄露漏洞，攻击者可利用该漏洞获取敏感信息。
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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/4693390139849392205

漏洞名称	ZTE GoldenDB DDE 注入漏洞
危害级别	高(AV:N/AC:L/Au:M/C:C/I:C/A:C)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03 , <=6.1.03.10ZTE ZXCLOUD GoldenDB 7.2.01.01ZTE ZXCLOUD GoldenDB Lite7.2.01.01
CVE 编号	CVE-2025-46579
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在 DDE 注入漏洞，攻击者可利用该漏洞通过接口注入 DDE 表达式，当用户下载并打开受影响的文件时，可以执行 DDE 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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/10364676150916014 74

漏洞名称	ZTE GoldenDB SQL 注入漏洞（CNVD-2025-10854）
危害级别	中(AV:L/AC:L/Au:S/C:C/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03 , <=6.1.03.10ZTE ZXCLOUD GoldenDB 7.2.01.01ZTE ZXCLOUD GoldenDB

	Lite7.2.01.01
CVE 编号	CVE-2025-46578
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在 SQL 注入漏洞，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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/4693390139849392210

漏洞名称	ZTE GoldenDB SQL 注入漏洞
危害级别	中(AV:N/AC:L/Au:S/C:C/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03 ， <=6.1.03.10ZTE ZXCLOUD GoldenDB 7.2.01.01
CVE 编号	CVE-2025-46577
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在 SQL 注入漏洞，该漏洞源于应用缺少对外部输入 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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/10364676150916014 69

4、Google 产品安全漏洞

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-10931）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android 12.1Google Android 12.0Google Android 13.0Google Android 14.0Google Android 15.0
CVE 编号	CVE-2024-40651
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提升权限。
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 代码执行漏洞（CNVD-2025-10930）
危害级别	高(AV:A/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android 12.0Google Android 13.0Google Android 12.1Google Android 14.0Google Android 15.0
CVE 编号	CVE-2024-43770

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，该漏洞是由于系统组件中的缺陷引起的。攻击者可利用发漏洞在系统上执行任意代码。
漏洞解决方案	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://source.android.com/docs/security/bulletin/2025-01-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2025-10929）
危害级别	中(AV:L/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Google Android 13.0Google Android 12.0Google Android 12.1Google Android 14.0Google Android 15.0
CVE 编号	CVE-2024-49742
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，该漏洞源于程序未正确检查权限，攻击者可利用该漏洞提升权限。
漏洞解决方案	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://source.android.com/docs/security/bulletin/2025-01-01

漏洞名称	Google Chrome 代码执行漏洞（CNVD-2025-10928）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <136.0.7103.92
CVE 编号	CVE-2025-4372
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导致堆损坏。
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/2025/05/stable-channel-update-for-desktop.html

漏洞名称	Google Chrome 安全绕过漏洞（CNVD-2025-10927）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Google Chrome <135.0.7049.52
CVE 编号	CVE-2025-3072
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 存在安全绕过漏洞，该漏洞源于 Custom Tabs 中的不当实现。攻击者可利用该漏洞绕过安全限制。
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/2025/04/stable-channel-update-for-desktop.html

漏洞名称	Google Chrome 安全绕过漏洞（CNVD-2025-10926）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Google Chrome <135.0.7049.52
CVE 编号	CVE-2025-3074
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 存在安全绕过漏洞，该漏洞源于 Downloads 中的不当实现。攻击者可利用该漏洞绕过安全限制。
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/2025/04/stable-channel-update-for-desktop.html

漏洞名称	Google Chrome 安全绕过漏洞（CNVD-2025-10925）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Google Chrome <135.0.7049.52
CVE 编号	CVE-2025-3073
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 存在安全绕过漏洞，该漏洞源于 Autofill 中的不当实现。攻击者可利用该漏洞绕过安全限制。
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/2025/04/stable-channel-update-for-desktop.html

漏洞名称	Google Chrome 安全绕过漏洞（CNVD-2025-10924）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Google Chrome <137.0.7151.55
CVE 编号	CVE-2025-5065
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 存在安全绕过漏洞，该漏洞是由于 FileSystemAccess API 中的不适当实现，攻击者可利用该漏洞通过特制的 HTML 页面执行用户界面欺骗。
漏洞解决方案	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://chromereleases.googleblog.com/2025/05/early-stable-update-for-desktop.html

5、D-Link DIR-600L formEasySetupWizard3 函数缓冲区溢出漏洞

漏洞名称	D-Link DIR-600L formEasySetupWizard3 函数缓冲区溢出漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	D-Link DIR-600L <=2.07B01
CVE 编号	CVE-2025-4342
漏洞描述	D-Link DIR-600L 是中国友讯（D-Link）公司的一个入门级无线路由器，支持 150Mbps 无线传输和 4 个百兆有线端口。D-Link DIR-

	600L 存在缓冲区溢出漏洞，该漏洞源于函数 formEasySetupWizard3 的参数 host 未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。
漏洞解决方案	目前厂商尚未发布升级程序修复该安全问题，详情见厂商官网：http://www.dlink.com.cn/

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 Connect 跨站脚本漏洞（CNVD-2025-10674）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Adobe Adobe Connect <=12.8
CVE 编号	CVE-2025-30315
漏洞描述	Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Connect 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript。
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/connect/apsb25-36.html

漏洞名称	Adobe Connect 跨站脚本漏洞（CNVD-2025-10676）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Connect <=12.8
CVE 编号	CVE-2025-30316
漏洞描述	Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Connect 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript。
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/connect/apsb25-36.html

漏洞名称	Microsoft Excel 代码执行漏洞（CNVD-2025-10609）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Excel 2016 Microsoft Office Online Server Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-27751
漏洞描述	Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Excel 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27751

漏洞名称	Microsoft Excel 代码执行漏洞（CNVD-2025-10610）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Excel 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024
CVE 编号	CVE-2025-27750
漏洞描述	Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Excel 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	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-27750

漏洞名称	NETGEAR RAX30 缓冲区溢出漏洞
危害级别	高(AV:A/AC:L/Au:N/C:C/I:C/A:C)
影响产品	NETGEAR NETGEAR RAX30 <1.0.12.100_HOTFIX

CVE 编号	CVE-2023-51635
漏洞描述	NETGEAR RAX30 是美国网件（NETGEAR）公司的一个双频无线路由器。NETGEAR RAX30 存在缓冲区溢出漏洞，该漏洞源于缺乏对用户提供的数据长度进行验证，攻击者可利用该漏洞执行任意代码。
漏洞解决方案	目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://kb.netgear.com/000065928/Security-Advisory-for-Multiple-Vulnerabilities-on-the-RAX30-PSV-2023-0139

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 NC Cloud 存在 SQL 注入漏洞
危害级别	中(AV:N/AC:H/Au:S/C:C/I:N/A:N)
影响产品	用友网络科技股份有限公司 NC Cloud
CVE 编号	无
漏洞描述	NC Cloud 是一款大型企业数字化平台，支持公有云、混合云、专属云的灵活部署模式。用友网络科技股份有限公司 NC 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，建议用户下载使用：https://security.yonyou.com/#/noticeInfo?id=432

漏洞名称	ZTE GoldenDB SQL 注入漏洞

危害级别	中(AV:N/AC:L/Au:S/C:C/I:N/A:N)
影响产品	ZTE ZXCLOUD GoldenDB >=6.1.03 , <=6.1.03.10ZTE ZXCLOUD GoldenDB 7.2.01.01
CVE 编号	CVE-2025-46577
漏洞描述	ZTE GoldenDB 是中国中兴通讯（ZTE）公司的一款金融级交易型分布式数据库。用于金融、政企、电信等行业，提供高可用数据服务。ZTE GoldenDB 存在 SQL 注入漏洞，该漏洞源于应用缺少对外部输入 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://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/10364676150916014 69

漏洞名称	Huawei EMUI 和 HarmonyOS 绕过权限检验漏洞
危害级别	中(AV:L/AC:L/Au:S/C:N/I:N/A:C)
影响产品	Huawei EMUI 12.0.0Huawei HarmonyOS 3.0.0Huawei HarmonyOS 2.1.0Huawei HarmonyOS 2.0.0Huawei HarmonyOS 3.1.0Huawei EMUI 13.0.0Huawei HarmonyOS 4.0.0Huawei HarmonyOS 4.2.0Huawei EMUI 14.0.0Huawei HarmonyOS 4.3.0
CVE 编号	CVE-2024-58044

漏洞描述	Huawei EMUI 是一款基于 Android 开发的移动端操作系统。Huawei HarmonyOS 是一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei EMUI 和 HarmonyOS 存在绕过权限检验漏洞，攻击者可利用该漏洞导致可用性受影响。
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://consumer.huawei.com/en/support/bulletin/2025/3/

漏洞名称	Huawei HarmonyOS 未授权访问漏洞
危害级别	中(AV:L/AC:L/Au:S/C:C/I:C/A:N)
影响产品	Huawei HarmonyOS 5.0.0
CVE 编号	CVE-2025-46589
漏洞描述	Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。Huawei HarmonyOS 存在未授权访问漏洞，该漏洞源于应用锁模块未授权访问。攻击者可利用该漏洞验证和访问未经授权的资源。
漏洞解决方案	目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://consumer.huawei.com/cn/support/bulletin/2025/5/

漏洞名称	TOTOLINK A950RG 命令执行漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	TOTOLINK A950RG V4.1.2cu.5204_B20210112
CVE 编号	CVE-2025-45798

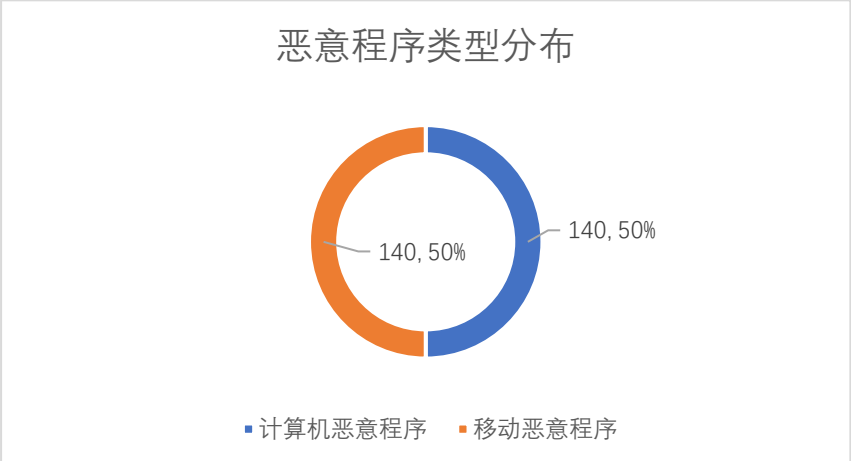
漏洞描述	TOTOLINK A950RG 是中国吉翁电子（TOTOLINK）公司的一款超世代 Giga 无线路由器。TOTOLINK A950RG 存在命令执行漏洞，该漏洞源于/lib/cste_modules/system.so 中 setNoticeCfg 接口 IpTo 参数未能正确过滤构造命令特殊字符、命令等。攻击者可利用该漏洞执行任意命令。
漏洞解决方案	目前厂商尚未发布升级程序修复该安全问题，详情见厂商官网：https://www.totolink.net/

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
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Packed.Win32.Krap.in	Win32	2025-06-01
Packed.Win32.Krap.in	Win32	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01

Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01
Trojan-PSW.MSIL.Reline.gen	MSIL	2025-06-01

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.rogue.Hiddad.Vmvm	Android	2025-06-01
a.rogue.Hiddad.Vmvm	Android	2025-06-01
a.rogue.Jiagu.Vrya	Android	2025-06-01
a.rogue.Jiagu.Vrya	Android	2025-06-01
a.payment.Smsspy.Vu11	Android	2025-06-01
a.payment.Smsspy.Vu11	Android	2025-06-01
a.payment.Smforw.V9xb	Android	2025-06-01
a.payment.Smforw.V9xb	Android	2025-06-01
a.rogue.Agent.V8eg	Android	2025-06-01
a.rogue.Agent.V8eg	Android	2025-06-01
a.payment.Anmon.Vkri	Android	2025-06-01
a.payment.Anmon.Vkri	Android	2025-06-01
a.privacy.Agent.Vuvr	Android	2025-06-01

a.privacy.Agent.Vuvr	Android	2025-06-01
a.rogue.Dowgin.Vw7p	Android	2025-06-01
a.rogue.Dowgin.Vw7p	Android	2025-06-01
a.rogue.Agent.Vslg	Android	2025-06-01
a.rogue.Agent.Vslg	Android	2025-06-01
a.rogue.Obfus.V0r1	Android	2025-06-01
a.rogue.Obfus.V0r1	Android	2025-06-01

2. 安全资讯

2.1. 高通 Adreno GPU 零日漏洞遭利用，全球安卓用户面临攻击风险

移动芯片制造商高通（Qualcomm）近日紧急发布安全补丁，修复其 Adreno GPU 驱动程序中三个正在被积极利用的关键零日漏洞（zero-day vulnerability），这些漏洞已被用于针对全球安卓用户的定向攻击。

被标记为 CVE-2025-21479 和 CVE-2025-21480 的两个漏洞属于高危漏洞，CVSS 评分为 8.6 分，属于图形组件中的授权错误缺陷。攻击者可通过特定命令序列在 GPU 微码中执行未授权命令，导致内存损坏，可能引发权限提升和系统沦陷。

第三个漏洞 CVE-2025-27038 的 CVSS 评分为 7.5 分，是图形组件中的释放后使用（use-after-free）漏洞。该漏洞主要影响 Chrome 浏览器中的 Adreno GPU 驱动渲染过程，可被利用来绕过浏览器隔离机制，在目标系统上执行任意代码。

这些漏洞影响深远，全球数十亿使用高通 Adreno GPU 技术的安卓设备面临风险，涉及三星、谷歌、小米和一加等多个智能手机品牌。高通已于 2025 年 5 月向原始设备制造商（OEM）分发补丁，并强烈建议立即部署。

2.2. Python 与 NPM 软件包中的后门程序同时威胁 Windows 和 Linux 系统

Checkmarx Zero 最新研究揭露了一场针对 Windows 和 Linux 系统 Python 与 NPM 用户的独特恶意软件攻击活动。

Checkmarx Zero 安全研究员 Ariel Harush 发现了这一令人担忧的网络攻击新趋势。根据其与 Hackread.com 共享的研究报告，攻击者正利用 "typosquatting"（域名抢注）和名称混淆技术诱骗用户下载恶意软件。该活动的特殊之处在于其跨生态系统攻击手法——攻击者将恶意软件包上传至 PyPI（Python 软件包索引），同时仿冒两个不同编程生态中的合法软件名称：colorama（Python 终端文本着色工具）和 colorizr（NPM 平台同类 JavaScript 包）。这种利用一个平台名称攻击另一平台用户的策略极为罕见。

Checkmarx Zero 发现的恶意软件包携带高危载荷，可使攻击者获得对桌面和服务器系统的持久远程访问与控制权，从而实现"敏感数据收集与渗出"。在 Windows 系统上，该恶意软件会尝试绕过杀毒软件检测。研究人员还发现部分 Windows 载荷关联至 GitHub 账户 githubcom/s7bhme。针对 Linux 用户的恶意软件包则包含高级后门，可建立加密连接、窃取信息并在受感染系统中长期隐蔽驻留。

由于缺乏明确归因数据，这场可能针对特定目标的攻击活动目前难以追踪，尚不确定是否与知名黑客组织有关。值得庆幸的是，相关恶意软件包已从公共软件仓库下架，暂时遏制了其破坏力。但 Checkmarx 仍建议各组织防范类似攻击。

2.3. 解析 Rootkit 技术原理、攻击手法与真实世界威胁

Rootkits 是一类旨在隐藏自身、其他恶意软件及其活动，并维持对受感染计算机系统未经授权访问的恶意软件。它们得名于“root”（Unix/Linux 系统中的最高管理员权限）和“kit”（工具包），本质上就是一套用于获取和保持高权限、同时不被发现的工具。

核心目标：隐蔽性、持久性、控制权。Rootkits 本身不是最终目标，而是实现其他恶意目的的手段。其使用动机包括：

1、维持持久访问：攻击者一旦入侵系统，就需要保持这种访问权限，即使系统重启、软件更新或用户尝试删除恶意软件。Rootkits 确保后门持续存在。

2、隐藏恶意活动：隐藏恶意进程：使恶意进程在任务管理器/ps 命令中不可见。隐藏恶意文件：使恶意文件、目录在文件浏览器/dir/ls 命令中不可见。隐藏恶意网络连接：使恶意软件建立的网络连接在 netstat 或类似工具中不可见。隐藏注册表项：(Windows) 隐藏恶意软件的配置或启动项。隐藏内核模块：(Linux/Unix) 隐藏恶意加载的内核模块。隐藏日志信息：篡改或阻止系统日志记录其活动。绕过安全软件：通过深度隐藏或直接干扰反病毒/反恶意软件、入侵检测系统（IDS）、防火墙的检测机制，使其难以发现或清除。窃取信息：在完全不被察觉的情况下，长期窃取敏感信息（如凭证、金融数据、个人隐私、商业机密）。建立僵尸网络：将受感染机器变成僵尸网络的一部分，用于发起分布式拒绝服务攻击、发送垃圾邮件、挖矿加密货币等，同时避免被用户或安全人员发现。间谍活动：针对特定目标进行长期监控。

2.4. Cursor 教育认证破解工具投毒风险，“薅羊毛”反被黑客组织窃密

近期，在日常监测安全动态时发现一起利用 AI 编程工具政策漏洞实施攻击的安全事件。事件起因于 AI 编程工具 Cursor 推出的“学生教育一年免费计划”，该计划明确将中国大陆地区用户排除在外，其前端地域校验机制又曾存在技术漏洞，因此这一情况迅速被不法分子所利用，在 GitHub 等平台上涌现了大量所谓的“Cursor 教育认证绕过工具”。值得警惕的是，其中部分传播的工具表面上声称可以帮助用户绕过地域限制，从而获取教育优惠，但实际上却暗藏恶意代码，目前已形成一套完整的攻击链条。

在此提醒广大用户，一定要通过官方渠道获取 Cursor 服务，切勿使用来源不明的程序，以免导致账号被盗或数据泄露，目前，火绒安全产品可对上述病毒进行拦截查杀，建议广大用户及时更新病毒库以提高防御能力。

2.5. 美国制裁涉 2 亿美元加密货币“杀猪盘”诈骗的 Funnull 公司

美国财政部外国资产控制办公室（OFAC）对菲律宾公司 Funnull Technology Inc.及其管理员实施制裁，指控该公司为"杀猪盘"骗局提供支持，导致美国受害者损失达 2 亿美元。

"杀猪盘"是一种网络诈骗形式，诈骗者通过建立虚假恋爱关系获取信任，最终实施经济剥削。犯罪者在建立网络恋爱关系后，会诱骗受害者转账或提供敏感财务信息，这些信息可能被用于其他欺诈活动。

Funnull Technology Inc.通过批量购买 IP 地址并转售给网络犯罪分子来支持加密货币骗局，这些 IP 被用于托管虚假交易平台。根据美国联邦调查局（FBI）报告，该公司与大多数诈骗案件有关联，造成美国受害者损失超过 2 亿美元。Funnull 使用域名生成算法和模板模仿正规网站以逃避关停。2024 年，该公司还篡改开发者代码，将用户重定向至与洗钱活动相关的诈骗和赌博网站。

美国财政部在声明中表示："Funnull Technology Inc.为数十万个涉及虚拟货币投资骗局（俗称'杀猪盘'）的网站提供计算机基础设施，与其管理员一同被列入制裁名单。2024 年这些网络犯罪收入创下历史新高，美国人每年因此损失数十亿美元。"

2.6. 微软与 CrowdStrike 合作建立统一威胁组织映射系统

CrowdStrike Holdings Inc.与微软公司今日宣布达成战略合作，旨在解决网络安全领域长期存在的威胁行为者跨平台识别与追踪标准混乱问题。该合作建立了共享映射系统，通过统一两家公司的威胁情报生态中的攻击者归属，消除因命名不一致导致的歧义。

网络安全行业长期面临一个典型问题：不同企业对同一威胁组织使用不同命名（例如 Cozy Bear 也被称为 Midnight Blizzard），这为情报追踪和行业协作制造了障碍。为此，双方开发了网络威胁情报的"罗塞塔石碑"系统，在不强制统一命名标准的前提下，实现跨供应商生态的攻击者标识符关联。

CrowdStrike 反攻击行动主管 Adam Meyers 指出："这是网络安全的分水岭时刻。攻击者不仅利用技术隐藏，还制造命名混乱来掩护自身行动。"微软安全副总裁 Vasu Jakkal 则强调，在 AI 驱动的新时代，这种合作能帮助防御者更快共享和响应威胁情报。未来两家公司计划持续扩展该计划，并邀请更多合作伙伴共建全球网络安全社区的威胁行为者映射资源。

2.7. HPE StoreOnce 软件曝出多个高危漏洞 攻击者可远程执行恶意代码

惠普企业(HPE)StoreOnce 软件平台存在多个安全漏洞，可能允许远程攻击者执行恶意代码、绕过认证机制并访问敏感企业数据。受影响版本包括 HPE StoreOnce VSA 4.3.11 之前的所有版本，这些漏洞对全球企业备份存储基础设施构成重大风险。

关键漏洞分析

1. **认证绕过漏洞(CVE-2025-37093)**：CVSS 3.1 评分 9.8（严重级），允许未认证攻击者完全绕过安全控制，获取存储系统未授权访问权限
2. **远程代码执行漏洞群**：包含 CVE-2025-37089/37091/37092/37096 (CVSS 7.2），高权限攻击者可利用 StoreOnce 架构缺陷远程执行任意代码，攻击向量标记为 AV（网络边界可触发）
3. **目录遍历漏洞**：CVE-2025-37094 (任意文件删除，CVSS 5.5）、CVE-2025-37095（信息泄露，CVSS 4.9），均通过路径操作缺陷实现攻击。

4. 技术特征

- 所有 RCE 漏洞均具备 CVSS:3.1/AV/AC/PR/UI/S/C/I/A 向量特征，表明其可导致系统完全沦陷
- AC（低攻击复杂度）评级意味着攻击者易于利用现成工具实施攻击

该漏洞集群由匿名研究人员与趋势科技 ZDI 团队协同发现，HPE 已发布修复方案。企业用户应立即升级至 4.3.11 或更高版本以消除风险。

2.8. 谷歌 Chrome 零日漏洞遭广泛利用，可执行任意代码

谷歌紧急修复 Chrome 零日漏洞 CVE-2025-5419，攻击者可利用 V8 引擎越界读写执行任意代码。已推送 137.0.7151.68/.69 版本更新，建议用户立即升级。漏洞正被活跃利用，属高优先级安全风险。

谷歌已发布 Chrome 浏览器紧急安全更新，确认编号为 CVE-2025-5419 的关键零日漏洞正被攻击者在野外活跃利用。该漏洞存在于 Chrome 的 V8 JavaScript 引擎中，攻击者可通过越界读写操作在受害者系统上执行任意代码。漏洞详情：

核心漏洞：CVE-2025-5419（CVSS 评分待公布）

类型：V8 引擎内存破坏漏洞

发现者：谷歌威胁分析小组 Clement Lecigne 与 Benoît Sevens（2025 年 5 月 27 日报告）

危害：允许远程代码执行（RCE），攻击者可窃取敏感数据或植入恶意代码

次级漏洞：CVE-2025-5068

类型：Blink 渲染引擎释放后重用漏洞

报告者：安全研究员 Walkman（获 1000 美元赏金）

危害：可能引发内存破坏及代码执行

谷歌暂未披露技术细节以防止漏洞被反向利用，其安全团队采用 AddressSanitizer 等工具强化防御体系。本次响应速度创历史纪录，凸显漏洞的极端危险性。

2.9. 高通 Adreno GPU 零日漏洞遭利用，全球安卓用户面临攻击风险

高通紧急修复 Adreno GPU 三个高危零日漏洞（CVE-2025-21479/21480/27038），全球数十亿安卓设备受影响。攻击者可利用漏洞执行任意代码或提升权限。补丁已发布，建议用户立即更新。事件凸显移动 GPU 安全挑战及行业协作重要性。

移动芯片制造商高通针对其 Adreno GPU 驱动中的三个高危零日漏洞发布紧急安全补丁，这些漏洞正被用于针对全球安卓用户的定向攻击。

漏洞关键信息

受影响组件：Adreno GPU 驱动

漏洞编号：

CVE-2025-21479

CVE-2025-21480

CVE-2025-27038

威胁等级：高危（存在定向攻击实例）

影响范围：搭载 Adreno GPU 的数十亿安卓设备，涵盖三星、谷歌、小米、一加等品牌。

2.10. Linux 核心转储漏洞可致敏感数据泄露

Linux 核心崩溃报告机制曝两处高危漏洞(CVE-2025-5054/4598)，影响 Ubuntu 和 RHEL 等主流系统，攻击者可窃取密码、密钥等敏感数据。建议临时禁用 SUID 核心转储功能缓解风险。

Qualys 威胁研究部门（TRU）最新披露发现两个本地信息泄露漏洞，影响主流 Linux 发行版的核心崩溃报告机制。这两个漏洞编号为 CVE-2025-5054 和 CVE-2025-4598，通过利用 Apport 和 systemd-coredump 组件中的竞争条件，可能使本地攻击者未经授权访问敏感系统内存。

首个漏洞（CVE-2025-5054）影响 Ubuntu 默认崩溃报告工具 Apport15，第二个漏洞（CVE-2025-4598）则针对 Red Hat Enterprise Linux (RHEL) 9/10、Fedora 40/41 及众多基于 systemd 的发行版广泛使用的 systemd-coredump 组件。

这两个漏洞均源于竞争条件——当系统行为依赖于不可控事件的时间顺序时产生的缺陷。攻击者可通过精确控制对 SUID 生成核心转储的访问时机，诱骗系统授予其本应仅限 root 用户读取的敏感文件访问权限。