天融信安全服务

安全通告

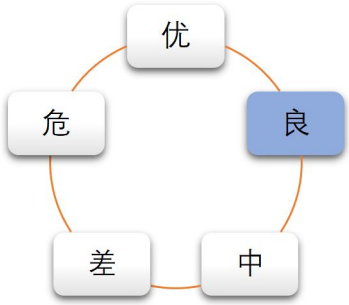
2025 年第 246 期（20250410）

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	10	21	0	0	0	9	2

1.2.3. 重要漏洞信息

1、IBM 产品安全漏洞

漏洞名称	IBM Security Verify Access 跨站脚本漏洞(CNVD-2025-06213)
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	IBM IBM Security Verify Access >=10.0.0，<=10.0.8
CVE 编号	CVE-2024-40700
漏洞描述	IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认

	证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Security Verify Access 存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，未经身份验证的攻击者可利用此漏洞在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期功能，导致受信任会话中的凭据泄露。
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://www.ibm.com/support/pages/node/7182386

漏洞名称	IBM Security Verify Access 跨站请求伪造漏洞
危害级别	高(AV:N/AC:L/Au:N/C:N/I:C/A:N)
影响产品	IBM IBM Security Verify Access >=10.0.0，<=10.0.8
CVE 编号	CVE-2024-35138
漏洞描述	IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Security Verify Access 存在跨站请求伪造漏洞，该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞执行从网站信任的用户传输的恶意和未经授权的操作。
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://www.ibm.com/support/pages/node/7182386

漏洞名称	IBM Security Verify Access 信息泄露漏洞(CNVD-2025-06210)
危害级别	中(AV:N/AC:H/Au:N/C:C/I:N/A:N)
影响产品	IBM IBM Security Verify Access >=10.0.0，<=10.0.8
CVE 编号	CVE-2024-43187
漏洞描述	IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Security Verify Access 存在信息泄露漏洞，该漏洞源于在通信通道中以明文形式传输敏感或安全关键数据，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://www.ibm.com/support/pages/node/7182386

漏洞名称	IBM Aspera Faspex 信息泄露漏洞（CNVD-2025-06209）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	IBM IBM Aspera Faspex >=5.0.0，<=5.0.10
CVE 编号	CVE-2023-37413
漏洞描述	IBM Aspera Faspex 是美国国际商业机器（IBM）公司的一种用于快速的全球个人对个人文件交付和协作的解决方案。IBM Aspera Faspex 存在信息泄露漏洞，该漏洞源于可观察到的响应差

	异，攻击者可利用该漏洞泄露敏感的用户名信息。
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://www.ibm.com/support/pages/node/7181814

漏洞名称	IBM ApplinX 跨站脚本漏洞（CNVD-2025-06208）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	IBM ApplinX 11.1
CVE 编号	CVE-2024-49792
漏洞描述	IBM ApplinX 是美国国际商业机器（IBM）公司的一个专注于将绿屏界面转换为基于 Web 的现代应用程序。IBM ApplinX 存在跨站脚本漏洞，攻击者可利用该漏洞在 Web UI 中嵌入任意 JavaScript 代码，导致可信会话中的凭据泄露。
漏洞解决方案	用户可参考如下厂商提供的信息以修复该漏洞：https://www.ibm.com/support/pages/node/7182522

漏洞名称	IBM ApplinX 跨站脚本漏洞（CNVD-2025-06207）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	IBM ApplinX 11.1
CVE 编号	CVE-2024-49793
漏洞描述	IBM ApplinX 是美国国际商业机器（IBM）公司的一个专注于将绿屏界面转换为基于 Web 的现代应用程序。IBM ApplinX 存在跨站脚本漏洞，攻击者可利用该漏洞在 Web UI 中嵌入任意 JavaScript

	代码，导致可信会话中的凭据泄露。
漏洞解决方案	用户可参考如下厂商提供的信息以修复该漏洞： https://www.ibm.com/support/pages/node/7182522

漏洞名称	IBM ApplinX 跨站请求伪造漏洞（CNVD-2025-06206）
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:N)
影响产品	IBM ApplinX 11.1
CVE 编号	CVE-2024-49794
漏洞描述	IBM ApplinX 是美国国际商业机器（IBM）公司的一个专注于将绿屏界面转换为基于 Web 的现代应用程序。IBM ApplinX 存在跨站请求伪造漏洞，攻击者可利用该漏洞构建恶意 URI，诱使请求，可以目标用户上下文执行恶意操作。
漏洞解决方案	用户可参考如下厂商提供的信息以修复该漏洞： https://www.ibm.com/support/pages/node/7182522

漏洞名称	IBM ApplinX 跨站请求伪造漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:N)
影响产品	IBM ApplinX 11.1
CVE 编号	CVE-2024-49795
漏洞描述	IBM ApplinX 是美国国际商业机器（IBM）公司的一个专注于将绿屏界面转换为基于 Web 的现代应用程序。IBM ApplinX 存在跨站请求伪造漏洞，攻击者可利用该漏洞构建恶意 URI，诱使请求，可

	以目标用户上下文执行恶意操作。
漏洞解决方案	用户可参考如下厂商提供的信息以修复该漏洞： https://www.ibm.com/support/pages/node/7182522

2、Xiaomi 产品安全漏洞

漏洞名称	Xiaomi AX1800 等命令注入漏洞
危害级别	高(AV:N/AC:L/Au:M/C:C/I:C/A:C)
影响产品	Xiaomi AX1800 rom <1.0.336 Xiaomi RM1800 root <1.0.26
CVE 编号	CVE-2020-14102
漏洞描述	Xiaomi AX1800 是中国小米公司的一款路由器。Xiaomi AX1800 等存在命令注入漏洞，攻击者可利用该漏洞提交特殊的请求，注入任意 OS 命令并执行。
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://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=23&locale=en

漏洞名称	Xiaomi Millet mobile phones 存在文件上传漏洞
危害级别	高(AV:N/AC:H/Au:N/C:C/I:C/A:N)

影响产品	Xiaomi Millet mobile phones 1-6.3.9.3
CVE 编号	CVE-2019-15843
漏洞描述	Xiaomi 手机是小米信息科技有限公司的一款智能手机。Xiaomi Millet mobile phones 存在文件上传漏洞。攻击者可利用该漏洞写入文件或读取特权数据。
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://www.mi.com

漏洞名称	Xiaomi Mi Sound 信息泄露漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Xiaomi Sound <=2.2.40
CVE 编号	CVE-2020-14126
漏洞描述	Xiaomi Mi Sound 是中国小米（Xiaomi）公司的一款智能音响 APP。 Xiaomi Mi Sound 存在信息泄露漏洞，该漏洞源于部分接口可以被远程调用，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程序修复该安全问题，详情见厂商官网 :https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=278

漏洞名称	Xiaomi router 命令注入漏洞（CNVD-2025-06298）
危害级别	中(AV:N/AC:H/Au:N/C:P/I:C/A:P)
影响产品	Xiaomi Xiaomi router <2023.2

CVE 编号	CVE-2023-26317
漏洞描述	Xiaomi router 是中国小米（Xiaomi）公司的一系列无线路由器。Xiaomi routers 存在命令注入漏洞，该漏洞源于对外接口返回的响应过滤不足，攻击者可以利用该漏洞通过劫持 ISP 或上层路由器来获取权限。
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://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=529

漏洞名称	Xiaomi Router 缓冲区溢出漏洞（CNVD-2025-06294）
危害级别	中(AV:L/AC:L/Au:M/C:C/I:C/A:C)
影响产品	Xiaomi Xiaomi router <2023.2
CVE 编号	CVE-2023-26318
漏洞描述	Xiaomi Router 是中国小米（Xiaomi）公司的一系列无线路由器。Xiaomi Router 存在缓冲区溢出漏洞，该漏洞源于应用在处理不受信任的输入时出现边界错误。攻击者可利用该漏洞执行任意代码或导致拒绝服务。
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://trust.mi.com/misrc/bulletins/advisory?cveId=539

漏洞名称	Xiaomi Router 命令注入漏洞（CNVD-2025-06295）
危害级别	中(AV:L/AC:L/Au:M/C:C/I:C/A:C)

影响产品	Xiaomi Xiaomi router <2023.2
CVE 编号	CVE-2023-26319
漏洞描述	Xiaomi router 是中国小米（Xiaomi）公司的一系列无线路由器。Xiaomi Router 存在命令注入漏洞，该漏洞源于未能正确过滤构造命令特殊字符。攻击者可利用该漏洞执行任意命令。
漏洞解决方案	目前厂商已发布升级程序修复该安全问题，详情见厂商官网:https://trust.mi.com/misrc/bulletins/advisory?cveId=536

漏洞名称	Xiaomi Router 命令注入漏洞（CNVD-2025-06296）
危害级别	高(AV:N/AC:H/Au:N/C:C/I:C/A:C)
影响产品	Xiaomi Xiaomi router <2023.2
CVE 编号	CVE-2023-26320
漏洞描述	Xiaomi Router 是中国小米（Xiaomi）公司的一系列无线路由器。Xiaomi Router 存在命令注入漏洞。漏洞是由于未充分筛选从外部接口返回的响应所致。攻击者可利用该漏洞获取路由器的权限。
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://trust.mi.com/misrc/bulletins/advisory?cveId=540

漏洞名称	Xiaomi GetApps 代码执行漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Xiaomi GetApps >=31.2.5.0，<32.0.0.1

CVE 编号	CVE-2023-26322
漏洞描述	Xiaomi GetApps 是中国小米（Xiaomi）公司的一个全球应用商店。Xiaomi GetApps 存在代码执行漏洞，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://trust.mi.com/misrc/bulletins/advisory?cveId=542

3、NVIDIA 产品安全漏洞

漏洞名称	NVIDIA SHIELD Experience 代码问题漏洞
危害级别	中(AV:L/AC:L/Au:N/C:N/I:N/A:C)
影响产品	NVIDIA SHIELD Experience <9.0
CVE 编号	CVE-2021-34405
漏洞描述	NVIDIA Shield Experience 是美国英伟达（Nvidia）公司的一款流媒体播放器。NVIDIA SHIELD Experience 存在代码问题漏洞，该漏洞源于 TrustZone 中的 NULL 指针取消引用错误而存在的。攻击者可利用该漏洞执行拒绝服务（DoS）攻击。
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://nvidia.custhelp.com/app/answers/detail/a_id/5259

漏洞名称	NVIDIA SHIELD Experience 资源管理错误漏洞

危害级别	中(AV:L/AC:L/Au:N/C:P/I:P/A:P)
影响产品	NVIDIA SHIELD Experience <9.0
CVE 编号	CVE-2021-34403
漏洞描述	NVIDIA Shield Experience 是美国英伟达（Nvidia）公司的一款流媒体播放器。NVIDIA SHIELD Experience 存在资源管理错误漏洞，该漏洞源于 nvmap ioctl 中的 use-after-free 错误而存在的。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://nvidia.custhelp.com/app/answers/detail/a_id/5259

漏洞名称	NVIDIA SHIELD Experience 访问控制错误漏洞
危害级别	中(AV:L/AC:L/Au:N/C:P/I:P/A:P)
影响产品	NVIDIA SHIELD Experience <9.0
CVE 编号	CVE-2021-34401
漏洞描述	NVIDIA SHIELD Experience 是美国英伟达（Nvidia）公司的一款流媒体播放器。NVIDIA SHIELD Experience 存在访问控制错误漏洞，该漏洞源于访问限制不当。攻击者可利用该漏洞导致拒绝服务。
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://nvidia.custhelp.com/app/answers/detail/a_id/5259

漏洞名称	NVIDIA SHIELD Experience 缓冲区溢出漏洞
危害级别	中(AV:L/AC:L/Au:N/C:P/I:P/A:P)

影响产品	NVIDIA SHIELD Experience <9.0
CVE 编号	CVE-2021-34402
漏洞描述	NVIDIA SHIELD Experience 是美国英伟达（Nvidia）公司的一款流媒体播放器。NVIDIA SHIELD Experience 存在缓冲区溢出漏洞，该漏洞源于 NVIDIA Tegra 内核驱动程序中的 NVIDIA NVDEC 中的边界错误。 攻击者可利用该漏洞触发内存损坏并执行任意代码。
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://nvidia.custhelp.com/app/answers/detail/a_id/5259

漏洞名称	NVIDIA vGPU Software 代码问题漏洞
危害级别	中(AV:L/AC:L/Au:N/C:N/I:N/A:C)
影响产品	NVIDIA vGPU Software
CVE 编号	CVE-2022-31618
漏洞描述	NVIDIA vGPU Software 是美国英伟达（NVIDIA）公司的一个用于为虚拟机提供 GPU 功能的管理软件。NVIDIA vGPU software 存在代码问题漏洞，攻击者可利用该漏洞拒绝服务。
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://nvidia.custhelp.com/app/answers/detail/a_id/5383

漏洞名称	NVIDIA vGPU Software 资源管理错误漏洞
危害级别	中(AV:L/AC:H/Au:S/C:C/I:C/A:C)
影响产品	NVIDIA virtual gpu >=11.0，<11.8

	NVIDIA virtual gpu >=13.0，<13.3 NVIDIA virtual gpu 14.0 NVIDIA virtual gpu 14.1
CVE 编号	CVE-2022-31614
漏洞描述	NVIDIA vGPU Software 是美国英伟达（NVIDIA）公司的一个用于为虚拟机提供 GPU 功能的管理软件。NVIDIA vGPU Software 存在资源管理错误漏洞，该漏洞源于双重释放某些资源，攻击者可利用该漏洞导致拒绝服务、代码执行和信息泄露。
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://nvidia.custhelp.com/app/answers/detail/a_id/5383

漏洞名称	NVIDIA Riva riva_quickstart 访问控制错误漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:P)
影响产品	NVIDIA Riva
CVE 编号	CVE-2025-23243
漏洞描述	NVIDIA Riva 是 NVIDIA 发布的一个完全加速的对话式 AI 应用框架，用于构建使用端到端的多模态对话式 AI 服务。NVIDIA Riva riva_quickstart 存在访问控制错误漏洞，攻击者可利用该漏洞提交特殊的请求，导致数据篡改或拒绝服务。
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://nvidia.custhelp.com/app/answers/detail/a_id/5625

漏洞名称	NVIDIA Riva 访问控制错误漏洞
危害级别	高(AV:N/AC:L/Au:N/C:P/I:P/A:P)
影响产品	NVIDIA Riva
CVE 编号	CVE-2025-23242
漏洞描述	NVIDIA Riva 是 NVIDIA 发布的一个完全加速的对话式 AI 应用框架，用于构建使用端到端的多模态对话式 AI 服务。NVIDIA Riva 存在访问控制错误漏洞，攻击者可利用该漏洞篡改数据，造成服务拒绝或信息泄露。
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://nvidia.custhelp.com/app/answers/detail/a_id/5625

4、Adobe 产品安全漏洞

漏洞名称	Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2025-06310）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Acrobat reader
CVE 编号	CVE-2024-49530
漏洞描述	Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Acrobat

	Reader 存在安全漏洞，攻击者可利用该漏洞导致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/acrobat/apsb24-92.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06311）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-52835
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 版本及之前版本存在安全漏洞，攻击者可利用该漏洞在受害者的浏览器会话中执行任意代码。
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/experience-manager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞

	（CNVD-2025-06312）
危害级别	低(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-52838
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 版本及之前版本存在安全漏洞，攻击者利用该漏洞在受害者的浏览器会话中执行任意代码。
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/experience-manager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06306）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-53968
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决

	方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 及之前版本存在安全漏洞，该漏洞源于存在安全问题，攻击者可利用该漏洞在受害者浏览器会话中执行任意代码。
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/experience-manager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06307）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-53967
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 及之前版本存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞在受害者浏览器会话中执行任意代码。
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/experience-man

	ager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06308）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-53974
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 及之前版本存在跨站脚本漏洞，该漏洞源于受到存储型跨站脚本(XSS)漏洞的影响。攻击者可利用该漏洞将恶意脚本注入易受攻击的表单字段。
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://helpx.adobe.com/security/products/experience-manager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06304）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-53970

漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 及之前版本存在安全漏洞，该漏洞源于存在安全问题，攻击者可利用该漏洞向易受攻击的表单字段注入恶意脚本。
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/experience-manager/apsb24-69.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-06305）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	Adobe Adobe Experience Manager <=6.5.21
CVE 编号	CVE-2024-53969
漏洞描述	Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe Experience Manager 6.5.21 及之前版本存在安全漏洞，该漏洞源于存在安全问题，攻击者可利用该漏洞在受害者浏览器会话中执行任意代码。

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/experience-manager/apsb24-69.html

5、Tencent Libpag 缓冲区溢出漏洞

漏洞名称	Tencent Libpag 缓冲区溢出漏洞
危害级别	低(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Tencent Libpag v4.3
CVE 编号	CVE-2024-33078
漏洞描述	Tencent Libpag 是一款腾讯公司推出的动画库。Tencent Libpag 存在缓冲区溢出漏洞，攻击者可利用该漏洞提交特殊的请求，可使应用程序崩溃或以应用程序上下文执行任意代码。
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.tencent.com/

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 Illustrators 栈缓冲区溢出漏洞（CNVD-2025-06309）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Illustrators 29.1Adobe Illustrators <=28.7.3
CVE 编号	CVE-2025-21163
漏洞描述	Adobe Illustrator 是一款由 Adobe 公司开发的专业矢量图形设计软件，广泛应用于平面设计、插画创作、网页设计等领域。Adobe Illustrators 在 29.1、28.7.3 及之前版本中存在栈缓冲区溢出漏洞。该漏洞是由于受影响版本在处理文件时，未能正确验证输入数据的边界导致栈缓冲区溢出。攻击者可利用该漏洞在当前用户的上下文中执行任意代码。
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/illustrator/apsb25-11.html

漏洞名称	NVIDIA Riva riva_quickstart 访问控制错误漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:P)
影响产品	NVIDIA Riva
CVE 编号	CVE-2025-23243
漏洞描述	NVIDIA Riva 是 NVIDIA 发布的一个完全加速的对话式 AI 应用框架，用于构建使用端到端的多模态对话式 AI 服务。NVIDIA Riva riva_quickstart 存在访问控制错误漏洞，攻击者可利用该漏洞提交

	特殊的请求，导致数据篡改或拒绝服务。
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://nvidia.custhelp.com/app/answers/detail/a_id/5625

漏洞名称	IBM ApplinX 跨站请求伪造漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:N)
影响产品	IBM ApplinX 11.1
CVE 编号	CVE-2024-49795
漏洞描述	IBM ApplinX 是美国国际商业机器（IBM）公司的一个专注于将绿屏界面转换为基于 Web 的现代应用程序。IBM ApplinX 存在跨站请求伪造漏洞，攻击者可利用该漏洞构建恶意 URI，诱使请求，可以目标用户上下文执行恶意操作。
漏洞解决方案	用户可参考如下厂商提供的信息以修复该漏洞：https://www.ibm.com/support/pages/node/7182522

漏洞名称	Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2025-06310）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe Acrobat reader
CVE 编号	CVE-2024-49530
漏洞描述	Adobe Acrobat Reader 是美国奥多比 (Adobe) 公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Acrobat

	Reader 存在安全漏洞，攻击者可利用该漏洞导致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/acrobat/apsb24-92.html

漏洞名称	IBM Security Verify Access 信息泄露漏洞(CNVD-2025-06210)
危害级别	中(AV:N/AC:H/Au:N/C:C/I:N/A:N)
影响产品	IBM IBM Security Verify Access >=10.0.0，<=10.0.8
CVE 编号	CVE-2024-43187
漏洞描述	IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Security Verify Access 存在信息泄露漏洞，该漏洞源于在通信通道中以明文形式传输敏感或安全关键数据，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://www.ibm.com/support/pages/node/7182386

1.2.4.2. 境内厂商产品漏洞

漏洞名称	Xiaomi router 命令注入漏洞（CNVD-2025-06298）
危害级别	中(AV:N/AC:H/Au:N/C:P/I:C/A:P)
影响产品	Xiaomi Xiaomi router <2023.2
CVE 编号	CVE-2023-26317
漏洞描述	Xiaomi router 是中国小米（Xiaomi）公司的一系列无线路由器。Xiaomi routers 存在命令注入漏洞，该漏洞源于对外接口返回的响应过滤不足，攻击者可以利用该漏洞通过劫持 ISP 或上层路由器来获取权限。
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://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=529

漏洞名称	Huawei HarmonyOS media library 模块权限校验漏洞
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Huawei HarmonyOS 5.0.0
CVE 编号	CVE-2024-57954
漏洞描述	Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei HarmonyOS media library 模块存在权限校验漏洞，攻击者可利用该漏洞导致机密性受影响。

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/2025/2/

漏洞名称	Xiaomi cloud service Application 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	Xiaomi Xiaomi cloud service Application <=1.12.0.0.25
CVE 编号	CVE-2023-26316
漏洞描述	Xiaomi cloud service Application 是中国小米（Xiaomi）公司的一款云服务 APP。Xiaomi cloud service Application 存在跨站脚本漏洞，该漏洞源于白名单检查功能允许加载 javascript 协议，攻击者可以利用该漏洞窃取帐户的 cookie。
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://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=322

漏洞名称	佳能 Canon vb-c60 摄像头存在远程控制后门漏洞
危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	日本佳能 canon VB-C60 v1.1.3
CVE 编号	无
漏洞描述	日本佳能是一家致力于图像、光学和办公自动化产品的日本公司，产品包括照相机、摄像机、复印机、传真机、影像扫描器和打印机等。佳能（canon）vb-c60 摄像头存在远程控制后门漏洞，允许

	攻击者在无需身份认证的情况，向 image.cgi 发送带有特定参数的 get 请求，进而可控制摄像头上下，左右转动，调整焦距。
漏洞解决方案	用户可参考如下供应商提供的安全公告获得补丁信息：http://www.canon.com.cn/support/announce/products/an_2015-05-29.html

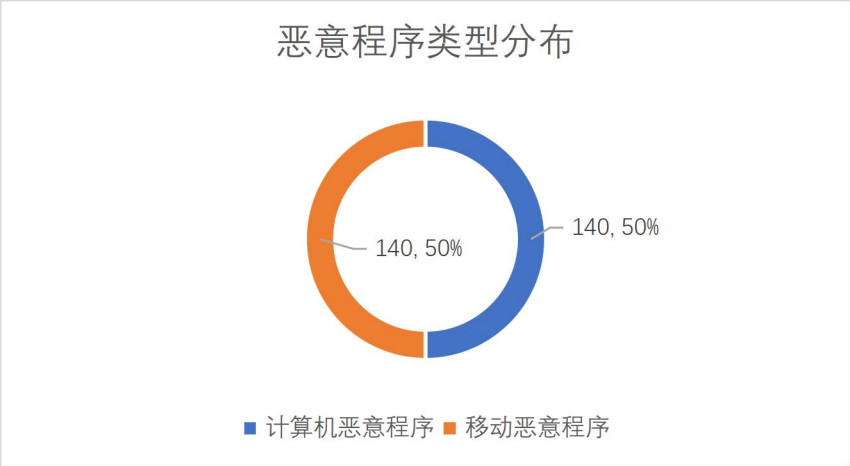
漏洞名称	Xiaomi GetApps 代码执行漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Xiaomi GetApps >=31.2.5.0，<32.0.0.1
CVE 编号	CVE-2023-26322
漏洞描述	Xiaomi GetApps 是中国小米（Xiaomi）公司的一个全球应用商店。Xiaomi GetApps 存在代码执行漏洞，攻击者可利用该漏洞执行任意代码。
漏洞解决方案	目前厂商已发布升级程序修复该安全问题，详情见厂商官网:https://trust.mi.com/misrc/bulletins/advisory?cveId=542

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
Virus.Win32.Ramnit.CD	Win32	2025-04-09
Virus.Win32.Ramnit.CD	Win32	2025-04-09
Trojan.Win32.Dynamer.bpb	Win32	2025-04-09
Trojan.Win32.Dynamer.bpb	Win32	2025-04-09
Adware.Win32.Agent.Gen	Win32	2025-04-09
Adware.Win32.Agent.Gen	Win32	2025-04-09
Trojan.Win32.Generic.ky	Win32	2025-04-09
Trojan.Win32.Generic.ky	Win32	2025-04-09
Trojan.Win32.VB.PQW	Win32	2025-04-09
Trojan.Win32.VB.PQW	Win32	2025-04-09

Backdoor.Win32.Fynloski.A	Win32	2025-04-09
Backdoor.Win32.Fynloski.A	Win32	2025-04-09
Trojan.Win32.Crypt.XPACK	Win32	2025-04-09
Trojan.Win32.Crypt.XPACK	Win32	2025-04-09
Rootkit.Win32.Agent.dqkh	Win32	2025-04-09
Rootkit.Win32.Agent.dqkh	Win32	2025-04-09
Worm.Win32.Soltern.oald	Win32	2025-04-09
Worm.Win32.Soltern.oald	Win32	2025-04-09
Trojan.Win32.VB.canh	Win32	2025-04-09
Trojan.Win32.VB.canh	Win32	2025-04-09

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.FakeAdBlocker.Vw28	Android	2025-04-09
a.rogue.FakeAdBlocker.Vw28	Android	2025-04-09
a.rogue.Hiddad.V5ym	Android	2025-04-09
a.rogue.Hiddad.V5ym	Android	2025-04-09
a.privacy.Hiddad.Vlkk	Android	2025-04-09
a.privacy.Hiddad.Vlkk	Android	2025-04-09
a.payment.Agent.V6tn	Android	2025-04-09

a.payment.Agent.V6tn	Android	2025-04-09
a.rogue.Fyben.V43k	Android	2025-04-09
a.rogue.Fyben.V43k	Android	2025-04-09
a.payment.Savestealer.Vzeo	Android	2025-04-09
a.payment.Savestealer.Vzeo	Android	2025-04-09
a.rogue.Agent.Veyv	Android	2025-04-09
a.rogue.Agent.Veyv	Android	2025-04-09
a.rogue.FakeAdBlocker.V3yc	Android	2025-04-09
a.rogue.FakeAdBlocker.V3yc	Android	2025-04-09
a.rogue.FakeAdBlocker.Vogt	Android	2025-04-09
a.rogue.FakeAdBlocker.Vogt	Android	2025-04-09
a.privacy.Hiddenapp.Vfqh	Android	2025-04-09
a.privacy.Hiddenapp.Vfqh	Android	2025-04-09

2. 安全资讯

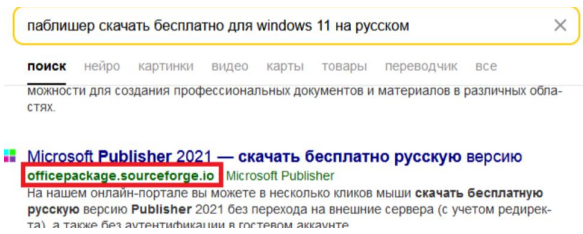
2.1. 黑客通过 SourceForge 分发伪装成微软 Office 插件的恶意软件

网络安全研究人员发现，攻击者正在滥用 SourceForge 平台分发伪装成微软插件的恶意工具，这些工具会在受害者电脑上安装同时具备挖矿和加密货币窃取功能的恶意软件。

SourceForge.net 是一个合法的软件托管和分发平台，支持版本控制、错误跟踪以及专用论坛/维基功能，因此在开源项目社区中非常受欢迎。虽然其开放的项目提交模式存在被滥用的风险，但实际通过该平台分发恶意软件的情况较为罕见。

卡巴斯基最新发现的这场攻击活动已影响超过 4,604 台系统，其中大部分位于俄罗斯。虽然该恶意项目已从 SourceForge 下架，但卡巴斯基表示搜索引擎仍保留着项目索引，导致搜索"office 插件"等关键词的用户仍可能被引导至恶意页面。

当用户在谷歌等搜索引擎中查找 Office 插件时，结果会指向"officepackage.sourceforge.io"——这是 SourceForge 为项目所有者提供的独立网页托管功能。该页面模仿了正规开发者工具页面，显示"Office 插件"和"下载"按钮。点击任何按钮后，受害者将获得一个包含密码保护压缩包(installer.zip)和密码文本文件的 ZIP 文件。



2.2. 利用 ChatGPT-4o 在 5 分钟内伪造护照 成功绕过 KYC 验证

波兰研究员 Borys Musielak 使用 ChatGPT-4o 在短短五分钟内生成了一份逼真的假护照。专家表示，该伪造文件足以通过自动化「了解你的客户」（KYC）验证流程。

"现在可以用 GPT-4o 生成假护照了。我只花了 5 分钟就制作出自己护照的复制件，大多数自动化 KYC 系统很可能不假思索就会接受。"Musielak 在 X 平台上发文称，"其影响显而易见——任何依赖图像作为'证据'的验证流程现在正式过时了。自拍验证同样如此，静态照片或动态视频都无关紧要，生成式 AI 也能伪造。基于照片的 KYC 验证已经终结。"

这份 AI 伪造的证件高度模仿真实护照，暴露出仅依赖照片和自拍匹配、缺乏芯片验证的数字身份识别系统存在重大缺陷。

Musielak 特别指出当前身份验证系统的脆弱性。与传统伪造手段不同，他规避了常见的 AI 生成缺陷，证明如今制作逼真伪造品的速度和便捷度已远超 Photoshop 等工具。

据科技媒体报道，使用 ChatGPT-4o 生成的假护照成功绕过了 Revolut 和 Binance 等金融科技平台采用的基础 KYC 检查——这些系统主要依赖身份证件照片上传和用户自拍验证。Musielak 警告称，随着生成式 AI 的普及，大规模身份盗用、欺诈性信贷申请和虚假账户注册等威胁正急剧增加。专家呼吁加强防御措施，包括推广基于 NFC 的验证技术和电子身份文件（eID），这些方案能提供更可靠的硬件级认证。

2.3. 谷歌发布网络安全 AI 新模型 Sec-Gemini v1

谷歌近日宣布推出实验性 AI 模型 Sec-Gemini v1，旨在通过人工智能技术革新网络安全防御体系。该模型由 Sec-Gemini 团队成员 Elie Burzstein 和 Marianna Tishchenko 共同研发，旨在帮助网络安全人员应对日益复杂的网络威胁。

Sec-Gemini 团队在博客中指出，网络安全领域长期存在固有的不对称性：防御方需要防范所有可能的攻击，而攻击者只需利用一个漏洞即可得手。这种失衡导致安全专业人员的工作既耗时又容易出错。Sec-Gemini v1 试图通过 AI 工具"倍增"网络安全工作流程的效率，将优势重新拉回防御方。

谷歌展示了该模型分析已知威胁组织"Salt Typhoon"的实例。Sec-Gemini v1 不仅准确识别出该威胁组织（这是许多 AI 模型无法做到的），还结合 Mandiant 威胁情报数据提供了详细描述。此外，该模型还分析了与 Salt Typhoon 相关的漏洞，从 OSV 数据库中提取数据并结合威胁组织背景信息进行深度解读。这种分析深度将帮助安全分析师更高效地评估风险并应对威胁。

谷歌强调，推进 AI 驱动的网络安全需要行业协同努力。为促进合作，Sec-Gemini v1 将免费向选定的组织、机构、专业人士和非政府组织开放用于研究目的。有意者可通过谷歌提供的表格申请早期访问权限。随着网络威胁不断演变，此类工具有望帮助防御方在与攻击者的对抗中占据更有利位置。

2.4. 新型恶意软件加载器采用调用栈欺骗、GitHub C2 与.NET Reactor 实现隐蔽攻击

网络安全研究人员发现名为 Hijack Loader 的恶意软件加载器推出新版本，通过新增功能逃避检测并在受感染系统中建立持久化驻留。Zscaler ThreatLabz 研究员 Muhammed Irfan V A 在分析报告中指出："Hijack Loader 新增调用栈欺骗模块，用于隐藏函数调用（如 API 和系统调用）的原始来源。该加载器还添加了反虚拟机检测模块，可识别恶意软件分析环境和沙箱。"

Hijack Loader 最早于 2023 年被发现，具备投放信息窃取类恶意软件等第二阶段有效载荷的能力。该加载器配备多种模块，可绕过安全软件并注入恶意代码。网络安全社区将其追踪为 DOILoader、GHOSTPULSE、IDAT Loader 和 SHADOWLADDER 等别名。

2024 年 10 月，HarfangLab 与 Elastic 安全实验室曾详细披露 Hijack Loader 攻击活动，其利用合法代码签名证书及臭名昭著的 ClickFix 策略进行传播。最新版本较前代有多项改进，最显著的是新增调用栈欺骗作为规避技术，隐藏 API 和系统调用的原始来源——这种技术近期也被另一款名为 CoffeeLoader 的恶意软件加载器采用。

Zscaler 解释称："该技术通过 EBP 指针链遍历堆栈，用伪造的堆栈帧替换真实堆栈帧，从而隐藏恶意调用痕迹。"与前代版本相同，Hijack Loader 仍采用 Heaven's Gate 技术执行 64 位直接系统调用以实现进程注入。其他改进包括更新进程黑名单，新增 Avast 杀毒软件组件"avastsvc.exe"，并将执行延迟设置为 5 秒。

2.5. 苹果 Vision Pro 曝出严重漏洞，黑客可通过用户眼动输入窃取信息

近日，苹果公司的 Vision Pro 混合现实头戴式设备曝出一个安全漏洞，一旦被黑客成功利用，他们就可以推断出用户在该设备的虚拟键盘上输入的具体数据。

该攻击活动名为 GAZEploit，该漏洞被追踪为 CVE-2024-40865。

佛罗里达大学的学者对此表示：这是一种新颖的攻击，因为攻击者可以从头像图片中推断出与眼睛有关的生物特征，从而重建通过注视控制输入的文本。GAZEploit 攻击利用了用户共享虚拟化身时凝视控制文本输入的固有漏洞。

在该漏洞披露后，苹果公司在 2024 年 7 月 29 日发布的 visionOS 1.3 中解决了这一问题。据苹果描述，该漏洞影响了一个名为 “Presence” 的组件。

该公司在一份安全公告中说：虚拟键盘的输入可能是从 Persona 中推断出来的，其主要通过 “在虚拟键盘激活时暂停 Persona” 来解决这个问题。

研究人员发现，黑客可以通过分析虚拟化身的眼球运动或 “凝视” 来确定佩戴该设备的用户在虚拟键盘上输入的内容，极易导致用户的隐私泄露。

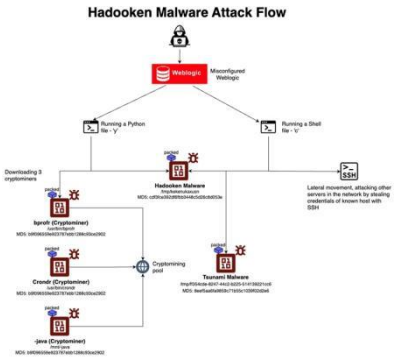
2.6. 只针对 Linux，甲骨文 Weblogic 服务器被黑客入侵

网络安全研究人员发现了一场针对 Linux 环境的新恶意软件活动，目的是进行非法加密货币挖矿和传播僵尸网络恶意软件。云安全公司 Aqua 指出，这项活动特别针对甲骨文 Weblogic 服务器，旨在传播一种名为 Hadooken 的恶意软件。

该恶意软件利用的是 Oracle Weblogic 中的一个已知漏洞，即 CVE-2020-14882。该漏洞允许攻击者获得对 Weblogic 服务器的未经授权访问，并执行任意代码。

安全研究员 Assaf Moran 表示，“当 Hadooken 行动被执行时，它会释放一种名为 Tsunami 的恶意软件，并部署一个加密货币挖矿程序来获取加密货币，如门罗币（XMR）。”

攻击链利用已知的安全漏洞和配置错误，例如弱密码，以获得初始立足点并在易受攻击的实例上执行任意代码。这是通过启动两个几乎相同的有效载荷来完成的，一个用 Python 编写，另一个是 shell 脚本，两者都负责从远程服务器（“89.185.85[.]102”或“185.174.136[.]204”）检索 Hadooken 恶意软件。



2.7. 新型 Vo1d 恶意软件曝光，超 130 万台安卓电视设备已中招

近日，有攻击者使用一种新的 Vo1d 后门恶意软件感染了 130 余万台安卓电视流媒体盒，使得攻击者能够完全控制这些设备。

Android TV 是谷歌针对智能电视和流媒体设备推出的操作系统，为电视和远程导航提供了优化的用户界面，集成了谷歌助手，内置 Chromecast，支持电视直播，并能安装应用程序。

该操作系统为包括 TCL、海信和 Vizio 电视在内的众多制造商提供智能电视功能。它还是英伟达 Shield 等独立电视流媒体设备的操作系统。

在 Dr.Web 的最新报告中，研究人员发现有 200 多个国家的 130 万台设备都感染了 Vo1 d 恶意软件，其中在巴西、摩洛哥、巴基斯坦、沙特阿拉伯、俄罗斯、阿根廷、厄瓜多尔、突尼斯、马来西亚、阿尔及利亚和印度尼西亚检测到的数量最多。

根据安装的 Vo1d 恶意软件版本，该活动将修改或替换操作系统文件，所有这些文件都是 Android TV 中常见的启动脚本。install-recovery.shdaemonsudebuggerd。

```
#!/system/bin/sh
func_start_kr() {
    /system/xbin/wd &
}

KR_TMP_FNAME=boxdaemon2
LOG_FILE_TMP=/data/local/tmp/$KR_TMP_FNAME.txt.tmp
LOG_FILE=/data/local/tmp/$KR_TMP_FNAME.txt
rm -f $LOG_FILE_TMP
rm -f $LOG_FILE
echo "[$0] begin ..." > $LOG_FILE_TMP
chmod 0777 $LOG_FILE_TMP
id >> $LOG_FILE_TMP  2>&1
func_start_kr >> $LOG_FILE_TMP 2>&1
echo "[$0] end!" >> $LOG_FILE_TMP
chcon u:object_r:shell_data_file:s0 $LOG_FILE_TMP
chown shell.shell $LOG_FILE_TMP
chmod 00644 $LOG_FILE_TMP
mv $LOG_FILE_TMP $LOG_FILE
```

2.8. 新型 PIXHELL 声音攻击能从 LCD 屏幕噪音中泄露信息

以色列内盖夫本古里安大学（Ben Gurion University of the Negev）的研究人员发现，一种被称为 “PIXHELL”的新型侧信道攻击可通过突破“音频间隙”攻击气隙系统（Air-gapped ）中的计算机，并利用屏幕上像素产生的噪声来窃取敏感信息。

所谓气隙系统是一种将电脑进行完全隔离（不与互联网以及任何其他联网设备连接)以保护数据安全的系统，通常是通过断开网线、禁用无线接口和 USB 连接来实现， 被认为是最难以渗透的、最安全的计算机。

该大学软件和信息系统工程系进攻性网络研究实验室（Offensive Cyber Research Lab）负责人 Mordechai Guri （莫迪凯·古里）博士在新发表的论文中称，气隙和音频气隙计算机中的恶意软件会生成精心制作的像素图案，产生频率范围在 0-22 千赫的噪声，恶意代码利用线圈和电容器产生的声音来控制从屏幕发出的频率，声音信号可以编码和传输敏感信息。

值得注意的是，这种攻击不需要任何专门的音频硬件、扬声器或被攻击计算机的内部扬声器，而是依靠 LCD 屏幕产生声音信号。

2.9. 为推送定制化广告，福特汽车新专利拟广泛采集驾驶员数据

据 The Cyber Express 消息，福特公司新申请的一项技术专利引发了人们对隐私问题的关注 ，该专利以推送定制化车载广告为目的，广泛收集驾驶员数据，包括车内对话。

批评者认为，这种侵入性的数据收集可能会导致有针对性的广告，让人感觉被操纵，甚至毛骨悚然，并对谁能访问这些数据以及如何确保数据安全表示担忧。《汽车影响》作者 Daryl Killian （达里尔·基利安）认为， 驾驶员可能会因此分心是另一个令人担忧的问题。 不断接收车载广告可能会转移驾驶员对道路的注意力，从而可能导致安全隐患。

然福特公司强调，申请专利并不能保证专利的最终实施。在给《财富》杂志的一份声明中，该公司称申请专利是探索新想法的一种标准做法，并不一定表示会发布这种系统。

不过，这并不是福特第一次探索个性化车载广告。 几年前，该公司申请了一项系统专利，当驾驶员开车经过广告牌时，会在车载显示屏上显示广告牌的数字版本。

2.10. Adobe 修复 ColdFusion 11 个高危漏洞 共修补 30 个安全缺陷

Adobe 近日发布安全更新，修复了包括 ColdFusion 2025、2023 和 2021 版本中多个高危漏洞在内的一系列安全问题，这些漏洞可能导致任意文件读取和代码执行。

在本次修复的 30 个漏洞中，11 个被评定为高危级别：

CVE-2025-24446（CVSS 评分：9.1）- 输入验证不当漏洞，可导致任意文件系统读取
CVE-2025-24447（CVSS 评分：9.1）- 不可信数据反序列化漏洞，可导致任意代码执行
CVE-2025-30281（CVSS 评分：9.1）- 访问控制不当漏洞，可导致任意文件系统读取
CVE-2025-30282（CVSS 评分：9.1）- 身份验证不当漏洞，可导致任意代码执行
CVE-2025-30284（CVSS 评分：8.0）- 不可信数据反序列化漏洞，可导致任意代码执行
CVE-2025-30285（CVSS 评分：8.0）- 不可信数据反序列化漏洞，可导致任意代码执行
CVE-2025-30286（CVSS 评分：8.0）- 操作系统命令注入漏洞，可导致任意代码执行
CVE-2025-30287（CVSS 评分：8.1）- 身份验证不当漏洞，可导致任意代码执行
CVE-2025-30288（CVSS 评分：7.8）- 访问控制不当漏洞，可导致安全功能绕过
CVE-2025-30289（CVSS 评分：7.5）- 操作系统命令注入漏洞，可导致任意代码执行
CVE-2025-30290（CVSS 评分：8.7）- 路径遍历漏洞，可导致安全功能绕过

Adobe 还发布了针对多款产品的修复补丁，包括：

After Effects（CVE-2025-27182、CVE-2025-27183）：修复越界写入和基于堆的缓冲区溢出漏洞
Media Encoder（CVE-2025-27194、CVE-2025-27195）：修复越界写入漏洞
Bridge（CVE-2025-27193）：修复越界写入漏洞
Premiere Pro（CVE-2025-27196）：修复越界写入漏洞
Photoshop（CVE-2025-27198）：修复越界写入漏洞
Animate（CVE-2025-27199）：修复越界写入漏洞
FrameMaker（CVE-2025-30304、CVE-2025-30297、CVE-2025-30295）：修复多个可能导致任意代码执行的漏洞。