天融信

安全通告

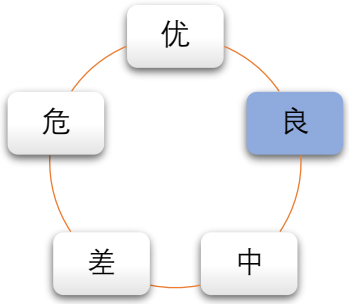
2025 年 8 月 6 日

目录

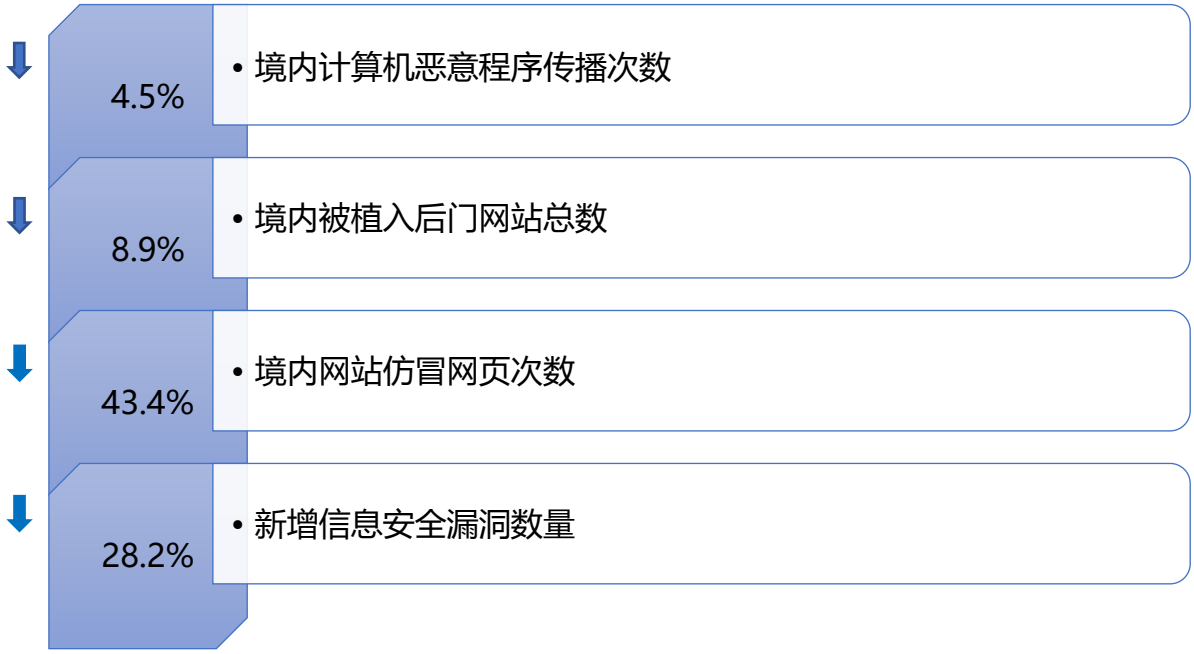
1. 安全态势

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：



---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	3	2	11	10	50	10	0

1.2.3. 重要漏洞信息

1、Microsoft 产品安全漏洞

漏洞名称	Microsoft Azure Functions 数据伪造问题漏洞
危害级别	高(AV:N/AC:H/Au:S/C:C/I:C/A:C)
影响产品	Microsoft Microsoft Azure Functions
CVE 编号	CVE-2025-33074
漏洞描述	Microsoft Azure Functions 是美国微软（Microsoft）公司的一个托管的平台即服务(PaaS) 提供程序，为 Azure 云服务提供事件驱动和计划的计算资源。Microsoft Azure Functions 存在

	数据伪造问题漏洞，该漏洞源于加密签名验证不当，攻击者可利用该漏洞可能导致远程代码执行。
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://azure.microsoft.com/en-us/products/functions

漏洞名称	Microsoft Azure Machine Learning 权限提升漏洞（CNVD-2025-17136）
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Microsoft Azure Machine Learning
CVE 编号	CVE-2025-49746
漏洞描述	Microsoft Azure Machine Learning 是美国微软（Microsoft）公司的机器学习服务平台。Microsoft Azure Machine Learning 存在安全漏洞，攻击者可利用该漏洞可能导致权限提升。
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49746

漏洞名称	Microsoft Azure DevOps 权限提升漏洞
危害级别	高(AV:N/AC:H/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Azure DevOps
CVE 编号	CVE-2025-47158

漏洞描述	Microsoft Azure DevOps 是美国微软（Microsoft）公司的一个团队协作服务平台。Microsoft Azure DevOps 存在安全漏洞，攻击者可利用该漏洞可能导致权限提升。
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47158

漏洞名称	Microsoft Azure Machine Learning 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	Microsoft Azure Machine Learning
CVE 编号	CVE-2025-49747
漏洞描述	Microsoft Azure Machine Learning 是美国微软（Microsoft）公司的机器学习服务平台。Microsoft Azure Machine Learning 存在安全漏洞，攻击者可利用该漏洞可能导致权限提升。
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49747

漏洞名称	Microsoft Windows 资源管理错误漏洞（CNVD-2025-16952）
危害级别	高(AV:N/AC:H/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Windows Server 2016 Microsoft Windows Server 2019

	Microsoft Windows Server 2012 Microsoft Windows Server 2022 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2025
CVE 编号	CVE-2025-49735
漏洞描述	Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。Microsoft Windows 存在安全漏洞。攻击者可利用该漏洞可以远程执行代码。
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49735

漏洞名称	Microsoft Windows 资源管理错误漏洞（CNVD-2025-16945）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Windows Server 2019 Microsoft Windows Server 2022 Microsoft Window 10 22H2 Microsoft Window 10 21H2 Microsoft Window 11 22H2 Microsoft Window 10 1809 Microsoft Window 11 23H2

	Microsoft Window 11 24H2 Microsoft Windows Server 2025
CVE 编号	CVE-2025-49724
漏洞描述	Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。Microsoft Windows 存在安全漏洞。攻击者可利用该漏洞可以远程执行代码。
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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49724

漏洞名称	Microsoft Excel 资源管理错误漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Microsoft Office Online Server Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC 2021 Microsoft Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024 Microsoft Excel 2016
CVE 编号	CVE-2025-49711
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 存在安全漏洞。攻击者利用该漏洞可以远程执行代码。

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49711

漏洞名称	Microsoft Office 资源管理错误漏洞（CNVD-2025-16943）
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-2025-49695
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 存在安全漏洞。攻击者可利用该漏洞可以远程执行代码。
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://msrc.microsoft.com/update-

	guide/vulnerability/CVE-2025-49695

2、IBM 产品安全漏洞

漏洞名称	IBM OpenPages with Watson 访问控制错误漏洞
危害级别	中(AV:N/AC:H/Au:N/C:N/I:C/A:N)
影响产品	IBM OpenPages with Watson 9.0 IBM OpenPages with Watson 8.3
CVE 编号	CVE-2025-27367
漏洞描述	IBM OpenPages with Watson 是 IBM 公司的一款企业级治理、风险和合规（GRC）管理平台。IBM OpenPages with Watson 8.3 和 9.0 版本存在安全漏洞，该漏洞源于当认证用户向服务器发送特制负载时，系统绕过了对 GRC 对象字段数据类型及必填项的客户端验证。攻击者可利用该漏洞绕过必填字段验证，导致数据在未存储必要字段的情况下被保存。
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://www.ibm.com/support/pages/node/7239155

漏洞名称	IBM Storage Virtualize 权限提升漏洞
危害级别	中(AV:L/AC:H/Au:S/C:C/I:C/A:C)

影响产品	IBM storage virtualize >=8.5，<=8.7
CVE 编号	CVE-2025-1351
漏洞描述	IBM Storage Virtualize 是 IBM 推出的企业级存储虚拟化产品，可实现跨异构存储系统的数据整合与管理。IBM Storage Virtualize 存在权限提升漏洞，该漏洞源于登录功能中的竞争条件问题。攻击者可利用该漏洞在同时登录场景下将自身权限提升至其他用户的权限级别。
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接：https://www.ibm.com/support/pages/node/7237157

漏洞名称	IBM Security QRadar Network Threat Analytics 资源管理错误漏洞
危害级别	中(AV:A/AC:L/Au:M/C:N/I:N/A:C)
影响产品	IBM Security QRadar Network Threat Analytics <=1.3.1
CVE 编号	CVE-2024-38335
漏洞描述	IBM Security QRadar Network Threat Analytics 是美国国际商业机器（IBM）公司的一款高级网络安全分析工具。IBM Security QRadar Network Threat Analytics 1.3.1 及之前版本存在资源管理错误漏洞，该漏洞源于资源分配不当，攻击者可利用该漏洞导致拒绝服务。

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://www.ibm.com/support/pages/node/7240244

漏洞名称	IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2025-17239)
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	IBM B2B Integrator >=6.0.0.0，<=6.1.2.6 IBM B2B Integrator >=6.2.0.0，<=6.2.0.4
CVE 编号	CVE-2025-2793
漏洞描述	IBM Sterling B2B Integrator 是 IBM 的企业级 B2B 集成平台，用于跨企业数据交换和业务流程自动化。IBM Sterling B2B Integrator 存在跨站脚本（XSS）漏洞，该漏洞源于未对用户输入的 JavaScript 代码进行有效过滤。攻击者可利用该漏洞通过认证后在 Web 界面嵌入恶意脚本，篡改预期功能，可能导致受信任会话中的凭证信息泄露。
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://www.ibm.com/support/pages/node/7239092

漏洞名称	IBM DB2 for Linux 拒绝服务漏洞
危害级别	中(AV:N/AC:H/Au:S/C:N/I:N/A:C)
影响产品	IBM DB2 for Linux 12.1.0

	IBM DB2 for Linux 12.1.1 IBM DB2 for Linux 12.1.2
CVE 编号	CVE-2025-2533
漏洞描述	IBM Db2 for Linux 是 IBM 开发的一款关系型数据库管理系统，专为 Linux 操作系统设计，提供高性能、高可靠性的数据存储和管理服务。IBM DB2 for Linux 存在拒绝服务漏洞，攻击者可利用该漏洞在处理特定构造的查询时导致服务器崩溃。
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.ibm.com/support/pages/node/7240947

漏洞名称	IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2025-16975）
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	IBM File Gateway >=6.0.0.0，<=6.1.2.6 IBM File Gateway >=6.2.0.0，<=6.2.0.4
CVE 编号	CVE-2025-3630
漏洞描述	IBM Sterling B2B Integrator 是 IBM 的企业级 B2B 集成平台，支持跨企业数据交换和业务流程自动化。IBM Sterling B2B Integrator 存在存储型跨站脚本（XSS）漏洞，该漏洞源于未对用户输入的 JavaScript 代码进行充分过滤。攻击者可利用该漏洞通过认证用户在 Web 界面中嵌入恶意脚本，篡改预期功能，

	可能导致受信任会话中的凭证信息泄露。
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://www.ibm.com/support/pages/node/7239095

漏洞名称	IBM Sterling File Gateway 信息泄露漏洞
危害级别	中(AV:N/AC:L/Au:S/C:P/I:N/A:N)
影响产品	IBM Sterling File Gateway >=6.0.0.0，<=6.1.2.6 IBM Sterling File Gateway >=6.2.0.0，<=6.2.0.4
CVE 编号	CVE-2025-2827
漏洞描述	IBM Sterling File Gateway 是 IBM 公司的一款企业级文件传输网关产品，用于安全可靠地管理和传输业务文件。IBM Sterling File Gateway 存在信息泄露漏洞，该漏洞源于系统向已认证用户暴露了敏感的安装目录信息。攻击者可利用该漏洞获取系统敏感路径信息，进而策划针对系统的进一步攻击。
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://www.ibm.com/support/pages/node/7239094

漏洞名称	IBM MQ 资源管理错误漏洞
危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	IBM MQ 9.3IBM MQ 9.4

CVE 编号	CVE-2025-3631
漏洞描述	IBM MQ 是 IBM 的企业级消息中间件，用于跨平台应用程序间的可靠通信。IBM MQ 9.3 及 9.4 版本存在通道进程崩溃漏洞，该漏洞源于客户端连接队列管理器时触发的 SIGSEGV 信号。攻击者可利用该漏洞通过特定客户端连接导致 AMQRMPPA 通道进程异常终止，引发拒绝服务。
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://www.ibm.com/support/pages/node/7238310

3、Adobe 产品安全漏洞

漏洞名称	Adobe InDesign 缓冲区溢出漏洞
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Adobe InDesign <=19.0 Adobe InDesign <=20.0
CVE 编号	CVE-2024-49529
漏洞描述	Adobe InDesign 是 Adobe 公司的一个桌面出版程序，主要用于各种印刷品的排版编辑。Adobe InDesign 存在缓冲区溢出漏洞，该漏洞源于存在越界读取问题，攻击者可利用该漏洞导致敏

	感内存泄露。
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://helpx.adobe.com/security/products/indesign/apsb24-91.html

漏洞名称	Adobe InDesign 越界读取漏洞
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Adobe InDesign <=ID19.5 Adobe InDesign <=ID18.5.3
CVE 编号	CVE-2024-49510
漏洞描述	Adobe InDesign 是 Adobe 公司的一个桌面出版应用程序，主要用于各种印刷品的排版编辑。Adobe InDesign 存在越界读取漏洞，该漏洞源于包含一个越界读取漏洞。攻击者可利用该漏洞导致敏感内存泄露。
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://helpx.adobe.com/security/products/indesign/apsb24-88.html

漏洞名称	Adobe InDesign Desktop 数字错误漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign Desktop <=19.5.3
CVE 编号	CVE-2025-47136

漏洞描述	Adobe InDesign Desktop 是 Adobe 公司开发的桌面出版软件，主要用于印刷品和数字出版物的排版设计，包括书籍、杂志、报纸、海报、电子书等。Adobe InDesign Desktop 存在数字错误漏洞，该漏洞源于整数值处理不当，攻击者可利用该漏洞提交特殊的文件请求，诱使用户解析，使应用程序崩溃或应用程序上下文执行任意代码。
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://helpx.adobe.com/security/products/indesign/apsb25-60.html

漏洞名称	Adobe ColdFusion 信任管理问题漏洞
危害级别	高(AV:A/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe ColdFusion <=2025.2 Adobe ColdFusion <=2023.14 Adobe ColdFusion <=2021.20
CVE 编号	CVE-2025-49551
漏洞描述	Adobe ColdFusion 是由 Adobe 公司维护的动态 Web 服务器平台。Adobe ColdFusion 存在信任管理问题漏洞，该漏洞源于硬编码凭证使用，攻击者可利用该漏洞导致权限提升。
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://helpx.adobe.com/security/products/coldfusion/ap

	sb25-69.html

漏洞名称	Adobe ColdFusion 代码问题漏洞
危害级别	高(AV:A/AC:L/Au:N/C:C/I:N/A:C)
影响产品	Adobe ColdFusion <=2025.2 Adobe ColdFusion <=2023.14 Adobe ColdFusion <=2021.20
CVE 编号	CVE-2025-49535
漏洞描述	Adobe ColdFusion 是由 Adobe 公司维护的动态 Web 服务器平台。Adobe ColdFusion 存在代码问题漏洞，该该漏洞源于 XML 外部实体引用限制不当，攻击者可利用该漏洞提交特殊的请求，获取敏感信息或进行拒绝服务攻击。
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://helpx.adobe.com/security/products/coldfusion/apsb25-69.html

漏洞名称	Adobe InDesign Desktop 缓冲区溢出漏洞
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Adobe InDesign Desktop <=19.5.3
CVE 编号	CVE-2025-43592
漏洞描述	Adobe InDesign Desktop 是 Adobe 公司开发的桌面出版软件，主要用于印刷品和数字出版物的排版设计，包括书籍、杂志、

	报纸、海报、电子书等。Adobe InDesign Desktop 存在缓冲区溢出漏洞，该漏洞源于访问未初始化指针，攻击者可利用该漏洞提交特殊的文件请求，诱使用户解析，使应用程序崩溃或应用程序上下文执行任意代码。
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://helpx.adobe.com/security/products/indesign/apsb25-60.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞
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 <=6.5.22
CVE 编号	CVE-2025-46959
漏洞描述	Adobe Experience Manager 是 Adobe 公司推出的企业级内容管理解决方案，旨在帮助企业高效构建、管理和交付多渠道数字内容与个性化体验。Adobe Experience Manager 存在跨站脚本漏洞，攻击者可利用该漏洞执行恶意 JavaScript 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://helpx.adobe.com/security/products/experience-manager/apsb25-48.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2025-17110）

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 <=6.5.22
CVE 编号	CVE-2025-47053
漏洞描述	Adobe Experience Manager 是 Adobe 公司推出的企业级内容管理解决方案，旨在帮助企业高效构建、管理和交付多渠道数字内容与个性化体验。Adobe Experience Manager 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	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://helpx.adobe.com/security/products/experience-manager/apsb25-48.html

4、Apache 产品安全漏洞

漏洞名称	Apache Commons Configuration 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 Apache Commons Configuration v1.x
CVE 编号	CVE-2025-46392
漏洞描述	Apache Commons Configuration 是美国阿帕奇（Apache）

	基金会的一款通用的配置接口，它主要用于使 Java 应用程序从多种来源读取配置数据。Apache Commons Configuration 1.x 版本存在资源管理错误漏洞，该漏洞源于未限制资源消耗，攻击者可利用该漏洞导致拒绝服务。
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://commons.apache.org/configuration/download_configuration.cgi

漏洞名称	Apache Tomcat 信息泄露漏洞（CNVD-2025-17251）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Apache Apache Tomcat
CVE 编号	CVE-2024-52317
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器，支持 Servlet 和 JavaServer Page（JSP）。Apache Tomcat 中存在信息泄露漏洞。该漏洞源于对象回收和重用不正确，可能导致用户之间的请求响应混淆。攻击者可以利用该漏洞获取其他用户的敏感信息。
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://lists.apache.org/thread/ty376mrxy1mmxtw3ogo53nc9l3co3dfs

漏洞名称	Apache Tomcat 拒绝服务漏洞（CNVD-2025-17252）

危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	Apache Tomcat >=9.0.76，<9.0.104 Apache Tomcat >=10.1.10，<10.1.40
CVE 编号	CVE-2025-31650
漏洞描述	Apache Tomcat 是一个免费的开放源代码的 Web 应用服务器。Apache Tomcat 存在安全漏洞，远程攻击者可以利用该漏洞提交特殊的请求，可使服务程序崩溃，造成拒绝服务攻击。
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://tomcat.apache.org/security-11.html

漏洞名称	Apache Tomcat 访问控制绕过漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Apache Tomcat >=10.1.0，<10.1.42 Apache Tomcat >=11.0.0，<11.0.8 Apache Tomcat >=9.0.0，<9.0.106
CVE 编号	CVE-2025-49125
漏洞描述	Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器，用于实现对 Servlet 和 JavaServer Page（JSP）的支持。Apache Tomcat 存在访问控制绕过漏洞，该漏洞源于使用 PreResources 或 PostResources 时可能绕过安全约束。攻击者可利用该漏洞通过绕过身份验证，访问未经授权的资源。

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://lists.apache.org/thread/m66cytbfrty9k7dc4cg6tl1czhsnbywk

漏洞名称	Apache Apisix 认证绕过漏洞
危害级别	中(AV:N/AC:H/Au:S/C:C/I:N/A:N)
影响产品	Apache APISIX <3.12.0
CVE 编号	CVE-2025-46647
漏洞描述	Apache Apisix 是美国阿帕奇（Apache）基金会的一个云原生的微服务 API 网关服务，该软件基于 OpenResty 和 etcd 来实现，具备动态路由和插件热加载，适合微服务体系下的 API 管理。Apache Apisix 存在认证绕过漏洞，该漏洞源于 openid-connect 插件在特定条件下可能允许跨发行者登录。攻击者可利用该漏洞通过获取系统内部的敏感信息，进一步扩大攻击范围。
漏洞解决方案	目前没有详细的解决方案提供：https://lists.apache.org/thread/yrpp2cd3o4qkxlrh421mq8gsrt0k4x0w

漏洞名称	Apache Guacamole 输入验证错误漏洞
危害级别	中(AV:N/AC:H/Au:S/C:C/I:C/A:N)
影响产品	Apache Guacamole <=1.5.5
CVE 编号	CVE-2024-35164

漏洞描述	Apache Guacamole 是美国阿帕奇（Apache）基金会的一款无客户端的远程桌面网关。该产品支持 VNC、RDP 和 SSH 等协议。Apache Guacamole 1.5.5 及之前版本存在输入验证错误漏洞，该漏洞源于未正确验证基于文本协议接收的控制台代码，攻击者可利用该漏洞导致执行任意代码。
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://guacamole.apache.org/

漏洞名称	Apache Jena 输入验证错误漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Apache Apache Jena <=5.4.0
CVE 编号	CVE-2025-50151
漏洞描述	Apache Jena 是 Apache 软件基金会的开源 Java 框架，用于构建语义网和链接数据应用。Apache Jena 5.4.0 及之前版本存在文件路径验证漏洞，该漏洞源于未对管理员上传的配置文件中的文件访问路径进行有效性校验。攻击者可利用该漏洞通过上传恶意配置文件实现任意文件访问。
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://lists.apache.org/thread/12gks5z40gh9bszn1xk8mz34gz586xss

漏洞名称	Apache Commons Lang 拒绝服务漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:N/A:P)
影响产品	Apache Commons Lang >=2.0，<2.6 Apache Commons Lang >=3.0，<3.18.0
CVE 编号	CVE-2025-48924
漏洞描述	Apache Commons Lang 是美国阿帕奇（Apache）基金会的一个工具库。Apache Commons Lang 存在拒绝服务漏洞，该漏洞源于 ClassUtils.getClass 方法存在无限递归，目前没有详细的漏洞细节提供。
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://commons.apache.org/proper/commons-lang/download_lang.cgi

5、MRCMS 跨站脚本漏洞（CNVD-2025-17130）

漏洞名称	MRCMS 跨站脚本漏洞（CNVD-2025-17130）
危害级别	低(AV:N/AC:L/Au:M/C:N/I:P/A:N)
影响产品	MRCMS MRCMS 3.1.3
CVE 编号	CVE-2025-4292
漏洞描述	MRCMS 是一款内容管理系统，用于管理和发布网站内容。

	MRCMS 3.1.3 中存在跨站脚本漏洞，受影响的是/admin/user/edit.do 文件中的编辑用户页面组件的未知功能。远程攻击者可利用该漏洞通过操控 Username 参数可导致跨站脚本攻击。
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://github.com/bdkuzma/vuln/issues/1

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	IrfanView CADImage Plugin 缓冲区溢出漏洞（CNVD-2025-17025）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	IrfanView CADImage Plugin 4.70
CVE 编号	CVE-2025-7250
漏洞描述	IrfanView CADImage Plugin 是 IrfanView 公司的一个 CAD 插件。IrfanView CADImage Plugin 存在缓冲区溢出漏洞，该漏洞源于解析 DWG 文件时缺乏对用户数据的验证，攻击者可利用该漏洞在当前进程的上下文中执行代码。
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://www.irfanview.com/

漏洞名称	WordPress structured content 跨站脚本漏洞
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	WordPress structured content <=1.6.4
CVE 编号	CVE-2025-4608
漏洞描述	WordPress structured content 是一种通过优化网页元素（如标题、描述、图片等）的语义化标记，提升搜索引擎对页面内容的理解能力，从而改善搜索结果展示和点击率的技术。WordPress structured content 存在跨站脚本漏洞，该漏洞源于输入清理和输出转义不足，攻击者可利用该漏洞通过跨站脚本攻击，篡改网页内容，误导用户。
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://wordpress.org/

漏洞名称	DELL NativeEdge 信息泄露漏洞
危害级别	中(AV:L/AC:L/Au:M/C:C/I:N/A:N)
影响产品	DELL NativeEdge 2.1.0.0
CVE 编号	CVE-2024-52543
漏洞描述	DELL NativeEdge 是戴尔科技推出的边缘运营软件平台，旨在简化边缘计算环境的部署、管理和安全扩展。DELL NativeEdge 存在信息泄露漏洞，该漏洞源于临时文件的权限设置不当。攻击

	者可利用该漏洞通过本地访问导致信息泄露。
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://www.dell.com/support/kbdoc/en-us/000258904/dsa-2024-488-security-update-for-dell-nativeedge-multiple-vulnerabilities

漏洞名称	WordPress User Registration Plugin 跨站脚本漏洞
危害级别	中(AV:N/AC:L/Au:S/C:P/I:P/A:N)
影响产品	WordPress User Registration Plugin <=4.2.4
CVE 编号	CVE-2025-6831
漏洞描述	WordPress User Registration Plugin 是一种用于扩展 WordPress 功能的插件，主要用于创建自定义用户注册表单、管理用户账户及实现会员制功能。WordPress User Registration Plugin 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	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://wordpress.org/plugins/user-registration/

漏洞名称	Oracle MySQL Server 资源管理错误漏洞（CNVD-2025-17178)
危害级别	中(AV:N/AC:L/Au:M/C:N/I:N/A:C)

影响产品	Oracle MySQL Server >=9.0.0，<=9.3.0 Oracle MySQL Server >=8.0.0，<=8.0.42 Oracle MySQL Server >=8.4.0，<=8.4.5
CVE 编号	CVE-2025-50091
漏洞描述	Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。Oracle MySQL Server 存在资源管理错误漏洞，该漏洞源于 Optimizer 组件访问控制不当，攻击者可利用该漏洞导致拒绝服务。
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://www.oracle.com/security-alerts/cpujul2025.html

1.2.4.2. 境内厂商产品漏洞

漏洞名称	Huawei HarmonyOS 拒绝服务漏洞（CNVD-2025-17360）
危害级别	中(AV:L/AC:L/Au:S/C:N/I:N/A:C)
影响产品	Huawei HarmonyOS 5.0.0
CVE 编号	CVE-2024-51519
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 存在拒绝服务漏洞，该漏洞源于 HDC 模块存在入参未安全校验。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/2024/11/

漏洞名称	Tenda FH1203 formQuickIndex 方法缓冲区溢出漏洞
危害级别	高(AV:N/AC:L/Au:S/C:C/I:C/A:C)
影响产品	Tenda FH1203 2.0.1.6
CVE 编号	CVE-2024-2993
漏洞描述	Tenda FH1203 是中国腾达推出的双频无线路由器，主要用于家庭网络覆盖。Tenda FH1203 存在缓冲区溢出漏洞，该漏洞源于/goform/QuickIndex 文件的 formQuickIndex 方法的 PPPOEPassword 参数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	目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://www.tenda.com.cn/download/detail-2495.html

漏洞名称	Huawei HarmonyOS 拒绝服务漏洞（CNVD-2025-17359）
危害级别	中(AV:L/AC:L/Au:S/C:N/I:N/A:C)
影响产品	Huawei HarmonyOS 5.0.0
CVE 编号	CVE-2024-51511
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 存在拒绝服务漏洞，该漏洞源于 WantAgent 模块存在传入类型校验缺失。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/2024/11/

漏洞名称	D-Link DIR-619L formTcpipSetup 函数缓冲区溢出漏洞
危害级别	中(AV:A/AC:L/Au:S/C:N/I:N/A:C)
影响产品	D-Link DIR-619L Rev.B 2.06B1
CVE 编号	CVE-2024-33772
漏洞描述	D-Link DIR-619L 是一款专为家庭及小型办公环境设计的无线路由器，采用 IEEE 802.11n 标准，最高传输速率达 300Mbps。D-Link DIR-619L 存在缓冲区溢出漏洞，该漏洞源于 formTcpipSetup 的参数 curTime 未能正确验证输入数据的长度大小，攻击者可利用该漏洞导致拒绝服务。
漏洞解决方案	目前厂商尚未发布升级程序修复该安全问题，详情见厂商官网：https://www.dlink.com/en

漏洞名称	Tenda AC10U formexeCommand 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	Tenda AC10U 15.03.06.49

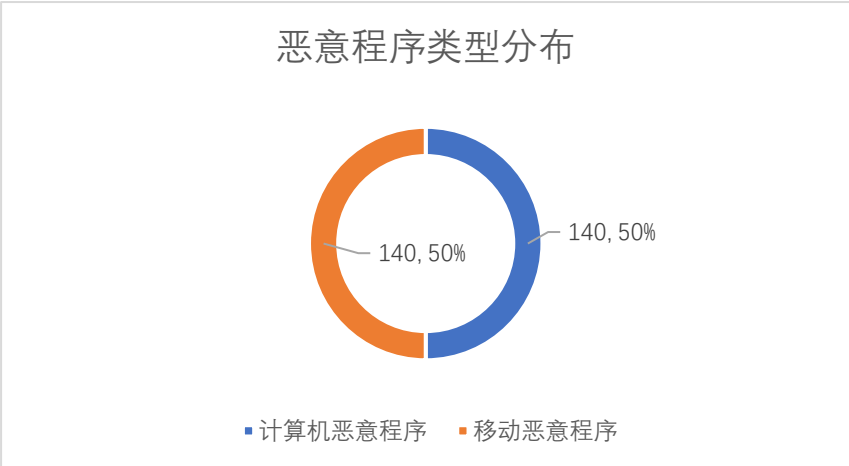
CVE 编号	CVE-2024-2708
漏洞描述	Tenda AC10U 是一款采用 802.11ac Wave 2.0 标准的双频千兆路由器，支持 MU-MIMO 技术，具备高穿墙能力和稳定传输特性。Tenda AC10U 存在缓冲区溢出漏洞，该漏洞源于 /goform/execCommand 文件的 formexeCommand 函数的 cmdinput 参数未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。
漏洞解决方案	目前厂商已发布升级程序修复该安全问题，详情见厂商官网：https://www.tendacn.com/download/detail-3170.html

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
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Riskware.Win32.CheatEngine.iszvqk	win7_sp1	2025-08-03
Riskware.Win32.CheatEngine.iszvqk	win7_sp1	2025-08-03
Mal/Generic-R	win7_sp1	2025-08-03
Mal/Generic-R	win7_sp1	2025-08-03
HackTool:Win32/CheatEngine.A!MTB	win7_sp1	2025-08-03
HackTool:Win32/CheatEngine.A!MTB	win7_sp1	2025-08-03
Trojan.Generic@ML.100 (RDMK:MzTRJvaBLCGSzj2aHZRDAA)	win7_sp1	2025-08-03

Trojan.Generic@ML.100 (RDMK:MzTRJvaBLCGSzj2aHZRDAA)	win7_sp1	2025-08-03
UDS:DangerousObject.Multi.Generic	win7_sp1	2025-08-03
UDS:DangerousObject.Multi.Generic	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03
Win32:Malware-gen	win7_sp1	2025-08-03

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.rogue.Agent.Vxce	Android	2025-08-03
a.rogue.Agent.Vxce	Android	2025-08-03
a.rogue.Agent.Vqqm	Android	2025-08-03
a.rogue.Agent.Vqqm	Android	2025-08-03
a.privacy.Metasploit.Vzn9	Android	2025-08-03

a.privacy.Metasploit.Vzn9	Android	2025-08-03
a.privacy.Hiddapp.Vxk8	Android	2025-08-03
a.privacy.Hiddapp.Vxk8	Android	2025-08-03
a.rogue.Obfus.Vh7x	Android	2025-08-03
a.rogue.Obfus.Vh7x	Android	2025-08-03
a.privacy.Metasploit.V7zp	Android	2025-08-03
a.privacy.Metasploit.V7zp	Android	2025-08-03
a.rogue.Hiddad.V1gs	Android	2025-08-03
a.rogue.Hiddad.V1gs	Android	2025-08-03
a.privacy.Metasploit.Vhgo	Android	2025-08-03
a.privacy.Metasploit.Vhgo	Android	2025-08-03
a.rogue.Dowgin.V88f	Android	2025-08-03
a.rogue.Dowgin.V88f	Android	2025-08-03
a.rogue.Clicker.Vu3v	Android	2025-08-03
a.rogue.Clicker.Vu3v	Android	2025-08-03

2. 安全资讯

2.1. 银狐钓鱼再升级：白文件脚本化实现 GO 语言后门持久驻留

历经两年的持续演进，银狐组织（SilverFox）采用的后门程序已从早期的 Gh0st、Win0s 等传统 RAT，发展成了多语言混合版本。

本次捕获的样本采用了 Go 语言编写，具备信息窃取、命令执行等基础恶意功能。值得注意的是，银狐组织的对抗技术也进行了显著升级：对此次样本的进程链进行分析发现，攻击者已经摒弃了早期依赖内存加载 PE 文件的方式，而是转用一种"白文件+脚本"的新型利用链——即利用合法 XML 文件配合 Python 脚本实施攻击。这种技术演进使得整个攻击过程中无需加载任何恶意 PE 文件(无任何黑 DLL，全文本攻击)，能够有效规避基于 ATT&CK 矩阵的常规检测手段，最终成功实现 Go 语言后门的持久化驻留。

而在溯源过程中发现，银狐组织已经能够通过单台服务器实现对上千台终端设备的控制。这些受控设备主要集中在财务、国企、政府等部门。银狐组织利用这些设备，通过企业微信、钉钉等即时通讯平台进一步下发信息，实施诈骗。

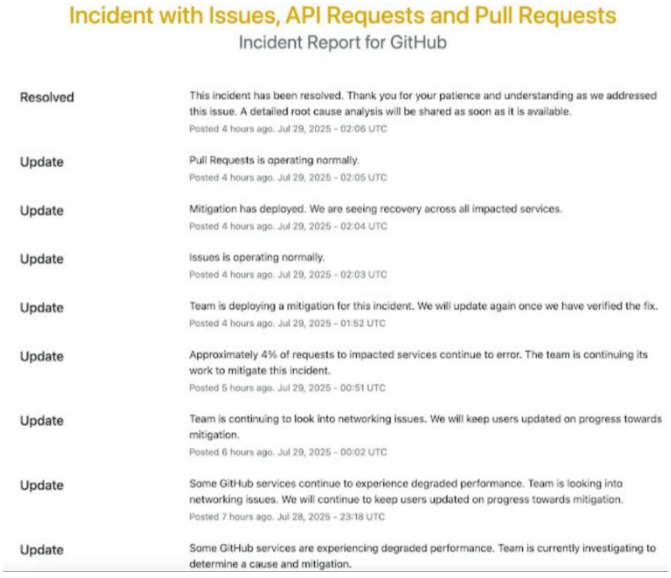
KeePass.exe 是一款开源的密码管理器，在该样本中被用作白利用程序。其通过附带的 KeePass.exe.config 配置文件实现 AppDomainManager 注入。

2.2. GitHub 全球核心服务中断事件全过程

2025 年 7 月 28 日，GitHub 发生大规模服务中断，影响全球数百万依赖该平台的开发者和组织。此次事件波及 API 请求、问题跟踪和拉取请求等核心功能，暴露出全球软件开发所依赖的云端协作工具的脆弱性。中断始于协调世界时 7 月 28 日 22:40，GitHub 状态页面随即报告这些核心功能性能下降。

从独立开发者到企业团队，全球用户均遭遇代码仓库访问、代码变更提交和项目管理等问题。此次中断正值关键时期——GitHub 支撑着从开源项目到科技巨头专有软件管道的各类业务。根据事件时间线，GitHub 工程团队在收到报告后立即展开调查，并于协调世界时 22:42 确认问题存在，开始排查潜在原因。

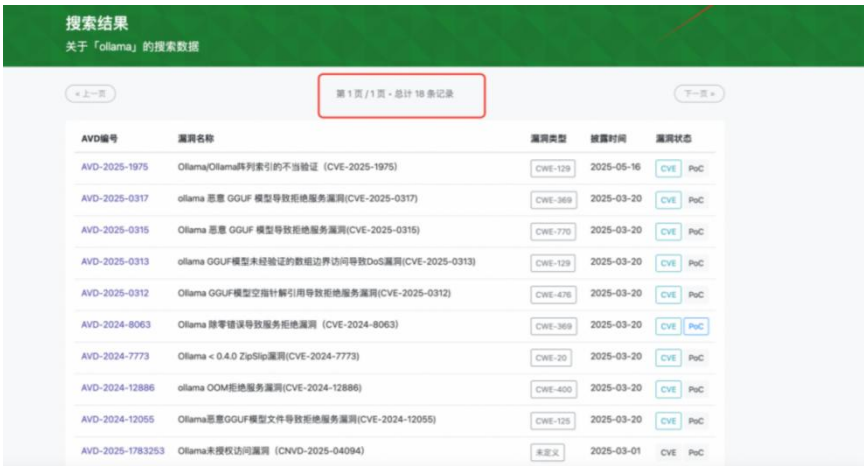
初步更新显示部分服务性能下降，团队认为网络问题可能是主要原因。随着时间进入 7 月 29 日，情况持续恶化。协调世界时 23:18 的更新指出性能仍在下降，至午夜时分，缓解工作聚焦于基础设施相关问题。虽然影响显著但有限——高峰期约 4%的请求出现错误，导致间歇性故障而非完全瘫痪。这种部分中断仍引发广泛不满，社交媒体上充斥着关于部署延迟和工作流中断的讨论。



2.3. Ollama 漏洞引发的“血案”—自建 LLM 的安全思考

通过网络空间安全测绘平台可以看到，截止 2025 年 7 月，全球仍然有 25 万个独立 IP 跟 Ollama 有关联，其中美国和中国分别占据前二的规模。由此可以看出自建 LLM 的情况仍然不少，并且扫描的端口中 11434（未授权访问漏洞关联的端口）比例依然很高。

Ollama 作为一款开源跨平台大语言模型（LLM）运行框架，因其轻量级设计、简化部署和跨平台支持（Windows、Linux、macOS）的特性，已成为 DeepSeek 等大模型部署的首选工具之一。该工具支持超过 1700 种模型的部署与管理，在 AI 研究和应用领域获得了广泛采用。然而，2025 年 3 月，国家网络安全通报中心发布了关于开源大模型工具 Ollama 的安全风险通报，其中最新的高危风险漏洞，漏洞编号：CNVD-2025-04094，其默认配置存在未授权访问隐患，导致未经授权的攻击者可在远程条件下调用 Ollama 服务接口，执行包括但不限于敏感模型资产窃取、虚假信息投喂、模型计算资源滥用和拒绝服务、系统配置篡改和扩大利用等恶意操作。



2.4. 全球蓝屏后，微软决定将安全踢出 Windows 内核

有消息称，微软正在重新设计 EDR 与 Windows 内核的交互方式，以避免再次引发全球蓝屏事件。

很明显，在 2024 年 7 月，由 CrowdStrike 故障引发的全球蓝屏事件给微软留下了极其深刻的记忆，从而促使后者进一步审视 EDR 在产品在设计和实施上的潜在风险，尤其是与内核交互的风险。

微软发文称，将在 Windows 11 中引入新的平台功能，并着重强调安全供应商在“内核模式之外”操作，以此避免类似事件的再次发生。因为微软已经无法再承受一次蓝屏事件的打击，需要确保 EDR 工具不会因为更新或者其他操作而导致整个系统的崩溃或者不稳定。

安全供应商在不进入内核模式的情况下运行安全产品，也有利于减少恶意软件利用内核漏洞的风险，提高整体系统的安全性。

虽然目前尚未公布具体细节，但是微软此次将“安全踢出 Windows 内核”的决心已经十分明显。

众所周知，在经历了越来越多的安全事件后，微软已在今年 8 月份提出“安全高于一切”的价值观，将安全工作与员工绩效评估联系起来，并把安全作为核心优先事项。微软副总裁 David Weston 也表示，这次重新设计将被视为实现长期韧性和安全目标的一部分。

这意味着微软不仅仅是在解决眼前的问题，而是在为未来的安全挑战做准备。由此也可以推测，安全产品将再也不会有机会重新进入 Windows 内核。

2.5. Twelve 黑客大肆攻击俄罗斯实体

据观察，一个名为 “Twelve ” 的黑客组织使用大量公开工具对俄罗斯目标实施破坏性网络攻击。

卡巴斯基在周五的分析中表示：与要求赎金解密数据不同，该组织更倾向于加密受害者的数据，然后使用擦除器破坏他们的基础设施，以防止恢复。

这表明，他们希望对目标组织造成最大程度的损害，而不是直接获得经济利益。

据悉，该黑客组织是在 2023 年 4 月俄乌战争爆发后成立的，曾发起过多次网络攻击事件、窃取敏感信息，然后通过其 Telegram 频道分享这些信息。

卡巴斯基称，Twelve 与一个名为 DARKSTAR（又名 COMET 或 Shadow）的勒索软件组织在基础架构和战术上有重合之处，因此这两个黑客组织很可能相互关联，或者是同一活动集群的一部分。

俄罗斯网络安全厂商说：Twelve 的行动明显具有黑客活动的性质，而 DARKSTAR 则坚持典型的双重勒索模式。集团内部目标的这种变化凸显了现代网络威胁的复杂性和多样性。

2.6. LockBit 勒索美国在线报税服务平台 eFile

据 The Cyber Express 消息，臭名昭著勒索软件组织 LockBit 于 9 月 18 日将美国在线报税服务 eFile.com 添加至受害者名单，要求在 14 天内支付赎金。eFile 为美国国税局（IRS）官方授权的税务申报平台。

人工智能驱动的威胁情报平台 Cyble 的研究人员表示，这次攻击 LockBit 没有发布任何文件，通常勒索软件都会释放一些所窃取数据的样例来印证其真实性。

目前，除了 14 天的赎金支付期限，有关 Lockbit 勒索软件攻击的程度、数据泄露以及网络攻击背后的动机的详细信息仍未披露。此外， eFile.com 官方网站仍然功能齐全。为了确认攻击的真实性，The Cyber Express 已经联系了 eFile 官员，目前尚未收到任何回复。

对于数百万依赖 eFile 报税的美国人来说，该服务一旦遭受攻击恐将面临潜在的严重。如果 LockBit 的攻击被证明属实，纳税人的个人和财务数据可能落入犯罪分子手中。这些数据可用于各种恶意活动，包括身份盗窃、税务欺诈和帐户接管。

2.7. Meta、YouTube 等巨头被曝长期监视未成年用户，牟利数十亿美元

根据美国联邦贸易委员会（FTC）工作人员的一份报告显示，社交媒体和视频流媒体公司一直在对用户，尤其是儿童和青少年进行广泛的监控，隐私保护不足，并通过数据货币化每年赚取数十亿美元。

此调查始于 2020 年 12 月，联邦贸易委员会于 2020 年 12 月公布了调查结果，并向亚马逊（Twitch 的所有者）、Meta（Facebook）、YouTube、Twitter（现为 X 公司）、Snapchat、TikTok（ByteDance 所有）、Discord、Reddit 和 WhatsApp（Meta）发出了命令。

这份报告调查了公司在 2019 年至 2020 年期间如何收集数据，追踪个人和人口统计信息，以及这些行为对未成年人造成了哪些影响。联邦贸易委员会今天公布的结果显示，这些做法在数据保留、数据共享和针对性广告方面引起了严重的担忧。

联邦贸易委员会（FTC）主席 Lina M. Khan 今日强调了这些调查结果的严重性，她指出报告揭露了这些公司如何将大量美国民众的个人资料转化为巨额利润，每年赚取数十亿美元。

2.8. Discord 推出端到端音频、视频加密通话功能

近日，Discord 推出了 DAVE 协议，这是一个定制的端到端加密（E2EE）协议，旨在保护平台上的音频和视频通话免遭未经授权的拦截。

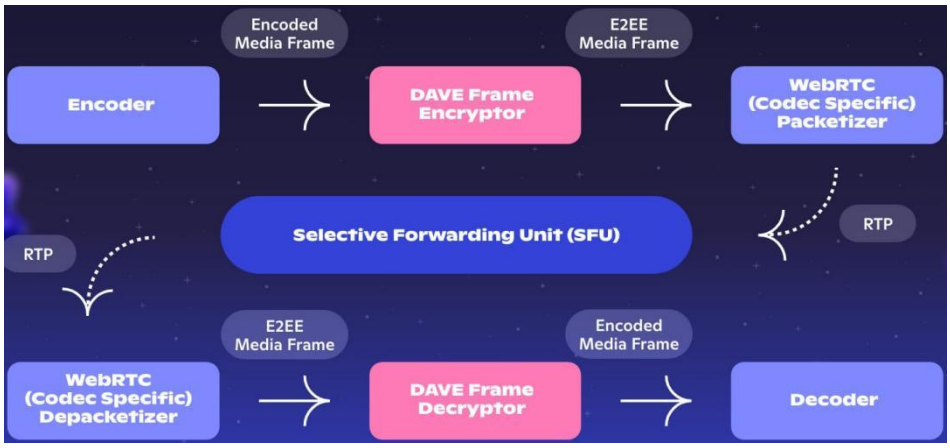
DAVE 是在 Trail of Bits 网络安全专家的帮助下创建的，该专家还对 E2EE 系统的代码和实施进行了审核。

新系统将涵盖用户在私人频道中的一对一音频和视频通话、小型群组聊天中的音频和视频通话、用于大型群组对话的基于服务器的语音频道以及实时流媒体。

Discord 在公告中写道： 他们将开始将 DM、群组 DM、语音频道和 Go Live 流中的语音和视频迁移至使用 E2EE。用户将能够确认通话何时进行了端到端加密，并对这些通话中的其他成员进行验证。

Discord 最初是为游戏玩家在游戏过程中进行交流而建立的，现在已发展成为世界上最流行的交流平台之一，满足了具有共同兴趣爱好的群体、创作者、企业和各种社区的需求。

最重要的是，Discord 决定将协议及其支持库开源，以便安全研究人员进行审查。此外，还发布了一份包含完整技术信息的白皮书，以确保对社区的透明度。



2.9. 黎巴嫩再发生爆炸事件，这次是对讲机

以色列新闻媒体称，贝鲁特的一家移动维修店和葬礼游行现场发生了爆炸。据黎巴嫩官方通讯社报道，贝鲁特和该国南部多个地区的房屋中还发生了太阳能系统爆炸，造成至少一名女孩受伤。

据 CNN 报道，黎巴嫩卫生部称，此次对讲机爆炸目前已造成至少 20 人死亡，其中包括一名 16 岁男孩，另有 450 多人受伤。

黎巴嫩通信部称，发生爆炸的 ICOM V82 型对讲机由日本公司 ICOM 生产，且该产品不是由公认的代理商提供，没有官方许可，也没有经过安全部门的审查。对此，ICOM 表示目前正在调查有关此事的事实。该公司网站称 IC-V82 已停产，目前流通的几乎所有型号都是假冒的。

根据《纽约时报》对现有视觉证据的分析，此次爆炸的对讲机比前一天在全国各地爆炸的寻呼机更大、更重，虽然爆炸发生地没有之前那么广泛，但在某些情况下还会引发更大的火灾，表明其中可能包含更多的爆炸物。

关于寻呼机、对讲机如何被引爆，目前说法不一。据央视新闻报道，有说法认为爆炸部件在制造或供应过程中被植入设备，也有人称操控者通过网络攻击导致设备电池过热爆炸。

2.10. 如何做好高校电子邮件账号安全防护

上个世纪七十年代，电子邮件占据了互联网的前身 ARPANET 上流量的 75%，是最主要的应用。随着互联网的发展，电子邮件在全面普及后，被各种各样的即时通讯软件抢走了不少风头。然而，其始终还是被社会所认可的主流网络通讯渠道，但是也成为最易被攻击的目标。当前电子邮件已经成为恶意连接、病毒木马的重要传播途径，研究发现网络安全事件中八成都和电子邮件有关。据 Cofense 的《2023 年度电子邮件安全报告》，2022 年全年恶意钓鱼电子邮件增加了 569%，与证书/凭据钓鱼相关的活跃威胁报告增加了 478%，恶意软件增加了 44%。商业电子邮件欺诈(BEC)连续第 8 年成为最严重的网络犯罪形式之一，在全球 90%的地区造成了机构数十亿美元的损失。利用人工智能、机器人进行信息窃取的恶意活动显著增加，攻击成本较低且快速有效，发起的混合攻击更难被检测和发现。

面对高校师生，对外的学术联系非常依赖电子邮件。如何保障好高校电子邮件账号的安全，确保研究人员对外学术联系的安全性、及时性、准确性，是值得电子邮件管理员关注的重要问题。可以在弄清威胁来源的基础上，及时发现并阻断入侵威胁，提升安全防护能力。

```
#!/bin/sh
# 配置参数
MAX_RECEIVER_COUNT=${1:-20} # 第一个参数，默认20
MAX_SEND_PER_DAY=${2:-3} # 第二个参数，默认3
SENDER_WHITE_LIST="./white.list"

# 相关变量
DATE=`date +'%Y%m%d'`
LOG_DATE=`date +'%Y_%m_%d'`
SENDER_INFO_FILE="${DATE}_batch_sender_info.list"
BATCH_SENDER_FILE="${DATE}_batch_sender_account.list"
BLOCK_SENDER_FILE="${DATE}_batch_sender_block.list"

# 搜索同时发送给20个及以上收件人的账号列表
grep "cmd:DATA.*\,Rcpt\:\(.*;\)\{$MAX_RECEIVER_COUNT,\}\,RcptHandle\:" /home/coremail1/cacgateway/logs/mtatrans/mta$LOG_DATE/*| awk
-F",Sender:" '{print $2}' | awk -F"," '{print $1}' | sort | uniq -c | sort -rnk1 > $SENDER_INFO_FILE

# 每天大批量发送邮件3次以上的列入待确认处理名单
awk -v MAX_SEND_PER_DAY=$MAX_SEND_PER_DAY '$1>=MAX_SEND_PER_DAY {print $2}' $SENDER_INFO_FILE > $BATCH_SENDER_FILE

# 去除白名单中的邮箱地址后，得到待处理名单block_sender.list
diff -u $SENDER_WHITE_LIST $BATCH_SENDER_FILE | grep '^\+[^+]' | cut -d'+' -f2 > $BLOCK_SENDER_FILE
cat $BLOCK_SENDER_FILE

# 封禁待处理名单
echo /home/coremail/bin/userutil --set-user-attr $BLOCK_SENDER_FILE user_status=1
/home/coremail/bin/userutil --set-user-attr $BLOCK_SENDER_FILE user_status=1
```