北京师范大学网络信息安全通告

2019 年 1 月报告

北京师范大学信息网络中心

2019 年 2 月

目录

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2019 年 1 月份采集安全漏洞共 1463 个。本月接报漏洞共计 5664 个，其中信息技术产品漏洞（通用型漏洞）65 个，网络信息系统漏洞（事件型漏洞）5599 个。

重大漏洞预警

1、ThinkPHP 5.0 远程代码执行漏洞（CNNVD-201901-445）：成功利用此漏洞的攻击者可以对目标系统进行远程代码执行攻击。ThinkPHP 5.0.x - 5.0.23 等多个版本均受此漏洞影响。目前，该漏洞的漏洞验证代码已经公开，同时 ThinkPHP 官方已经发布了该漏洞的修补措施，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

2、微软多个安全漏洞：微软官方发布了多个安全漏洞的公告，包括 Microsoft Windows 权限提升漏洞（CNNVD-201901-176、CVE-2019-0543）、Windows 内核信息泄漏漏洞（CNNVD-201901-137、CVE-2019-0536）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，采取修补措施。

1. 公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2019 年 1 月份新增安全漏洞共 1463 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 156 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 9.84%。本月新增漏洞中，超危漏洞 52 个、高危漏洞 122 个、中危漏洞 1072 个、低危漏洞 217 个，相应修复率分别为 86.54%、80.33%、54.94%以及 60.83%。合计 864 个漏洞已有修复补丁发布，本月整体修复率 59.06%。截至 2019 年 1 月 31 日，CNNVD 采集漏洞总量已达 121355 个。

1.1. 漏洞增长概况

2019 年 1 月新增安全漏洞 1463 个，与上月（1275 个）相比增加了 14.75%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1252 个。

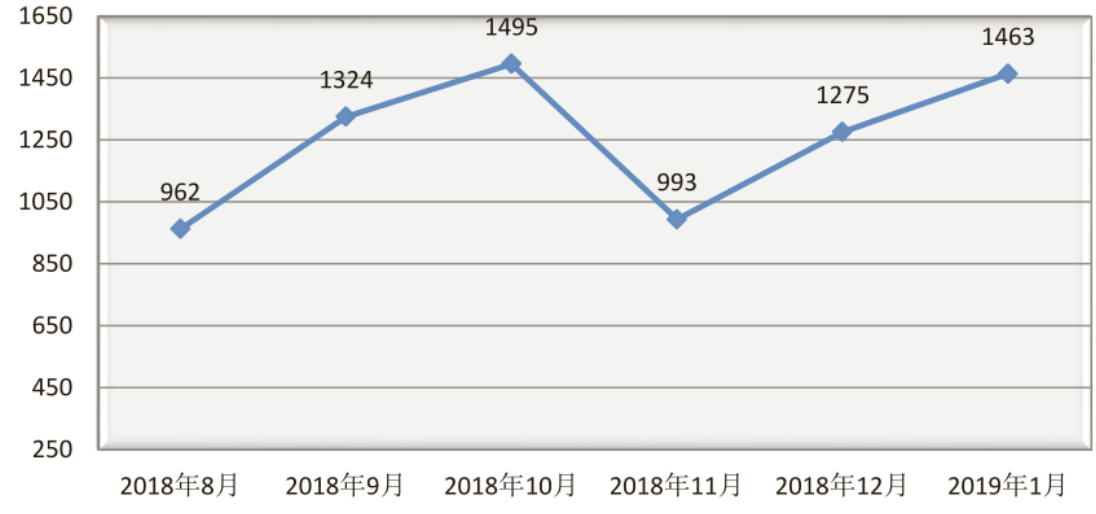

图 1 2018 年 8 月至 2019 年 1 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

1 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司达到 156 个，占本月漏洞总量的 10.66%。本月苹果、思科、CloudBees 等公司的漏洞数量均有所上升，Adobe、Google、IBM 等厂商的漏洞数量出现较不同程度的下降。

表1　2019 年 1 月新增安全漏洞排名前十厂商统计表

序号	厂商名称	漏洞数量	所占比例
1	Oracle	156	10.66%
2	苹果	68	4.65%
3	微软	52	3.55%
4	谷歌	48	3.28%
5	思科	45	3.08%
6	CloudBees	27	1.85%
7	JuniperNetworks	25	1.71%
8	福昕	20	1.37%
9	IBM	18	1.23%
10	NEC	17	1.16%

1.2.2. 漏洞产品分布

1 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 27 条，其中桌面操作系统 27 条，服务器操作系统 26 条。本月 Apple iOS 漏洞数量最多，达到 49 个，占主流操作系统漏洞总量的 17.56%，排名第一。

表 2　2019 年 1 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量

1	Apple iOS	49
2	Apple macOS High Sierra	38
3	Microsoft Windows 10	27
4	Microsoft Windows Server 2016	26
5	Microsoft Windows Server 1709	25
6	Microsoft Windows Server 2012	19
7	Microsoft Windows 8.1	19
8	Microsoft Windows Rt 8.1	19
9	Microsoft Windows Server 2008	16
10	Microsoft Windows 7	16
11	Android	16
12	Linux Kernel	9

说明：

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3. 漏洞类型分布

1 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 9.84%。

表3　2019 年 1 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	跨站脚本	144	9.84%

2	缓冲区错误	110	7.52%
3	信息泄露	56	3.83%
4	输入验证	56	3.83%
5	权限许可和访问控制	34	2.32%
6	SQL 注入	32	2.19%
7	跨站请求伪造	28	1.91%
8	操作系统命令注入	18	1.23%
9	资源管理错误	16	1.09%
10	路径遍历	15	1.03%
11	命令注入	15	1.03%
12	代码注入	10	0.68%
13	访问控制错误	10	0.68%
14	授权问题	8	0.55%
15	信任管理	7	0.48%
16	数字错误	5	0.34%
17	竞争条件	3	0.21%
18	配置错误	1	0.07%
19	加密问题	1	0.07%

1.2.4. 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。1 月漏洞危害等级分布如图 2 所示，其中超危漏洞 52 条，占本月漏洞总数的 3.55%。

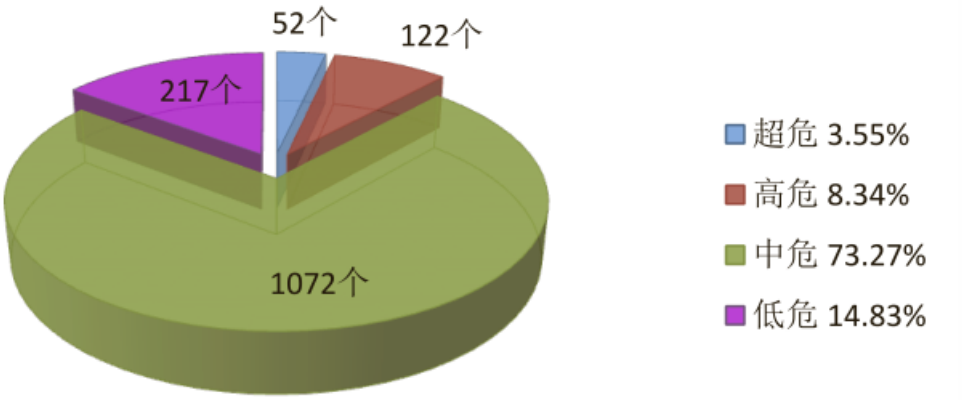

图 2　2019 年 1 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

1 月漏洞修复情况按危害等级进行统计见图 3。其中超危漏洞修复率最高，达到 86.54%，中危漏洞修复率最低，比例为 54.94%。与上月相比，本月超危、低危漏洞修复率有所上升，高危、中危漏洞修复率有所下降。总体来看，本月整体修复率下降，由上月的 74.90%下降至本月的 59.06%。

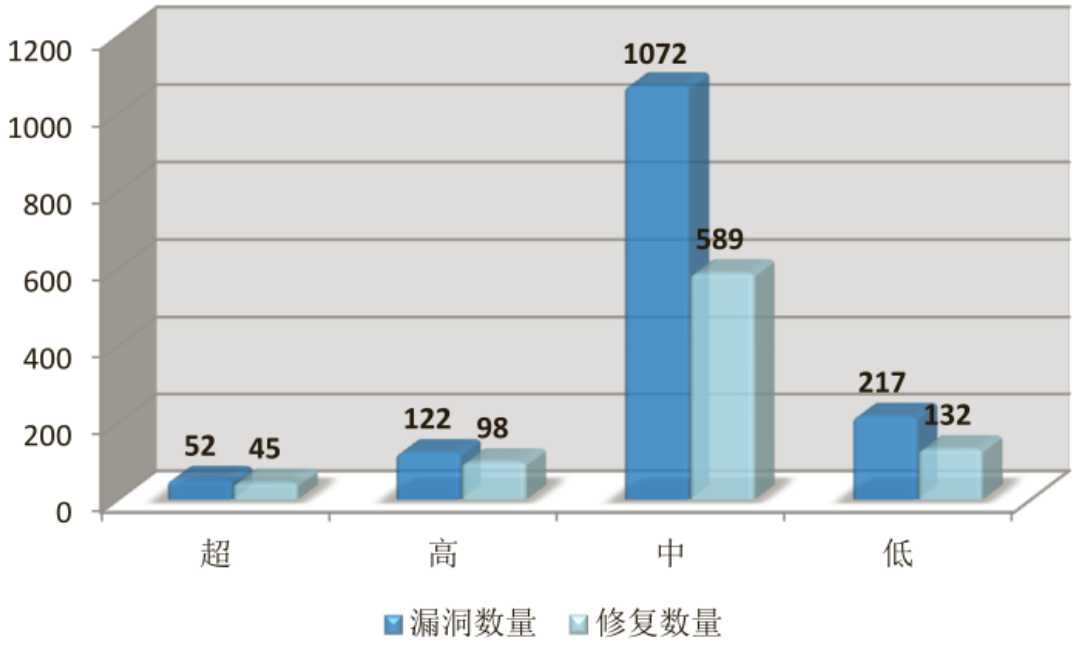

图 3　2019 年 1 月漏洞修复数量统计

1.3.2. 厂商修复情况

1 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、苹果、微软等十个厂商共 476 条漏洞，占本月漏洞总数的 32.54%，漏洞修复率为 100%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Oracle、苹果、微软、谷歌、思科、CloudBees、Juniper Networks、福昕、IBM、NEC 等公司本月漏洞修复率均为 100%，共 673 条漏洞已全部修复。

表 4 2019 年 1 月厂商修复情况统计表

序号	厂商名称	漏洞数量	修复数量	修复率
1	Oracle	156	156	100.00%
2	苹果	68	68	100.00%
3	微软	52	52	100.00%
4	谷歌	48	48	100.00%
5	思科	45	45	100.00%
6	CloudBees	27	27	100.00%
7	JuniperNetworks	25	25	100.00%
8	福昕	20	20	100.00%
9	IBM	18	18	100.00%
10	NEC	17	17	100.00%

1.4. 重要漏洞实例

1.4.1. 超危漏洞实例

本月超危漏洞共 52 个，其中重要漏洞实例如表 5 所示。

表 5 2019 年 1 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	操作系统命令	CNNVD-201901-027	友讯	NEC Aterm WG1200HP 操作系统命令注入漏洞

		CNNVD-201901-240 CNNVD-201901-241 CNNVD-201901-242 CNNVD-201901-243 CNNVD-201901-244 CNNVD-201901-245 CNNVD-201901-246 CNNVD-201901-249 CNNVD-201901-250 CNNVD-201901-251 CNNVD-201901-252 CNNVD-201901-253 CNNVD-201901-254	NEC	（CNNVD-201901-241）
2	缓冲区错误	CNNVD-201901-124 CNNVD-201901-125 CNNVD-201901-126 CNNVD-201901-127 CNNVD-201901-130 CNNVD-201901-133 CNNVD-201901-134 CNNVD-201901-146 CNNVD-201901-148 CNNVD-201901-149 CNNVD-201901-150 CNNVD-201901-174 CNNVD-201901-179	微软	Microsoft Exchange Server 缓冲区错误漏洞（CNNVD-201901-146）
		CNNVD-201901-383 CNNVD-201901-399 CNNVD-201901-411 CNNVD-201901-412	苹果	
		CNNVD-201901-851 CNNVD-201901-852 CNNVD-201901-853 CNNVD-201901-854 CNNVD-201901-855 CNNVD-201901-872	思科	
3	授权问题	CNNVD-201901-888	研华	Advantech WebAccess/SCADA 授权问题漏洞（CNNVD-201901-888）
4	输入验证	CNNVD-201901-147 CNNVD-201901-177	微软	Apple macOS High Sierra AMD 输入验证漏洞

		CNNVD-201901-408	苹果	（CNNVD-201901-408）

1. NEC Aterm WG1200HP 操作系统命令注入漏洞（CNNVD-201901-241）

NEC Aterm WG1200HP 是日本电气（NEC）公司的一款无线路由器。使用 1.0.31 及之前版本固件的 NEC Aterm WG1200HP 中存在操作系统命令注入漏洞。攻击者可利用该漏洞执行任意操作系统命令。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jpn.nec.com/security-info/secinfo/nv18-011.html

2. Microsoft Exchange Server 缓冲区错误漏洞（CNNVD- 201901-146）

Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序，它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。

Microsoft Exchange Server 中存在远程代码执行漏洞，该漏洞源于软件无法正确处理内存中的对象。远程攻击者可利用该漏洞在系统用户的上下文中运行任意代码。以下版本受到影响：

- Microsoft Exchange Server 2016 Cumulative Update 10
- Microsoft Exchange Server 2016 Cumulative Update 11
- Microsoft Exchange Server 2019

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0586

3. Advantech WebAccess/SCADA 授权问题漏洞（ CNNVD-201901-888 ）

Advantech WebAccess/SCADA 是研华（Advantech）公司的一套基于浏览器架构的 SCADA 软件。该软件支持动态图形显示和实时数据控制，并提供远程控制和管理自动化设备的功能。

Advantech WebAccess/SCADA 8.3 版本中存在授权问题漏洞。攻击者可利用该漏洞绕过身份验证，上传恶意数据。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接:

https://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download

4. Apple macOS High Sierra AMD 输入验证漏洞（ CNNVD-201901-408 ）

Apple macOS High Sierra 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。AMD 是其中的一个 AMD 产品组件。

Apple macOS High Sierra 10.13.4 版本中的 AMD 存在输入验证漏洞。攻击者可利用该漏洞以内核权限执行任意代码。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/zh-cn/HT208849。

1.4.2. 高危漏洞实例

本月高危漏洞共 122 个，其中重点漏洞实例如表 6 所示。。

表 6 2019 年 1 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL注入	CNNVD-201812-1183	Battelle MemorialInstitute	DevellionCubeCart SQL注入漏洞（CNNVD-201901-485）
		CNNVD-201812-1227	五指	
		CNNVD-201901-484	OXID	

			eSales	
		CNNVD-201901-485	Devellion	
2	代码注入	CNNVD-201901-136	SAP	SAP Cloud Connector 代码注入漏洞（CNNVD-201901-136）
		CNNVD-201901-512	LCDS	
		CNNVD-201901-736	Omron	
3	资源管理错误	CNNVD-201901-883	Google	Google Go 资源管理错误漏洞（CNNVD-201901-883）
4	信息泄露	CNNVD-201812-1172	Ansible	Cisco Small Business RV320 和RV325 信息泄露漏洞（CNNVD-201901-876）
		CNNVD-201901-876	Cisco	
5	授权问题	CNNVD-201901-120	SAP	CrestronAirMedia AM-100 授权问题漏洞（CNNVD-201901-750）
		CNNVD-201901-742	XytronixResearch&Design	
		CNNVD-201901-750	Crestron Electronics	
6	命令注入	CNNVD-201901-437	AudioCodes	Omron CX-Supervisor 命令注入漏洞（CNNVD-201901-738）
		CNNVD-201901-738	Omron	
		CNNVD-201901-877	Cisco	
7	权限许可和访问控制	CNNVD-201901-330	Symantec	Cisco SD-WAN Solution 权限许可和访问控制漏洞（CNNVD-201901-868）
		CNNVD-201901-349	Imperva	
		CNNVD-201901-387	Apple	
		CNNVD-201901-774	CA	
		CNNVD-201901-868 CNNVD-201901-870	Cisco	

8	缓冲区错误	CNNVD-201901-153 CNNVD-201901-154 CNNVD-201901-156 CNNVD-201901-173 CNNVD-201901-178	Microsoft	Microsoft Edge和ChakraCore缓冲区错误漏洞（CNNVD-201901-153）
		CNNVD-201901-522	wolfSSL	
		CNNVD-201901-758 CNNVD-201901-759 CNNVD-201901-760 CNNVD-201901-755	Qualcomm	
		CNNVD-201901-516 CNNVD-201901-514	LCDS	
		CNNVD-201901-809	Apple	
9	访问控制错误	CNNVD-201901-871	Cisco	Cisco SD-WAN SolutionvContainer 访问控制错误漏洞（CNNVD-201901-871）
		CNNVD-201901-098	Apache	
10	路径遍历	CNNVD-201901-604	MailEnable	MailEnable 路径遍历漏洞（CNNVD-201901-604）
11	输入验证	CNNVD-201901-170 CNNVD-201901-169	Microsoft	ABB CP400PB TextEditor 输入验证漏洞（CNNVD-201901-741）
		CNNVD-201901-869	Cisco	
		CNNVD-201901-741	ABB	
12	跨站脚本	CNNVD-201901-743	XytronixResearch&Design	XytronixResearch&DesignControl ByWeb X-320M 跨站脚本漏洞（CNNVD-201901-743）
13	竞争条件	CNNVD-201901-756	Qualcomm	多款 Qualcomm snapdragon 产品竞争条件漏洞（CNNVD-201901-756）
14	跨站请求伪造	CNNVD-201901-894	Phoenix Contact	Phoenix Contact FL SWITCH 跨站请求伪造漏洞（CNNVD-201901-894）

1. DevellionCubeCart SQL 注入漏洞（CNNVD-201901-485）

DevellionCubeCart 是英国 Devellion 公司的一套免费且开源的电子商务购物车软件。该软件支持在网上商店销售产品、添加/编辑产品或图像等。DevellionCubeCart 6.1.13 之前版本中存在 SQL 注入漏洞。远程攻击者可借助‘密码找回’功能的‘validate[]’参数利用该漏洞检索敏感的数据库信息。

解决措施：目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.cubecart.com/

2. SAP Cloud Connector 代码注入漏洞（CNNVD-201901-136）

SAP Cloud Connector 是德国思爱普（SAP）公司的一款用于连接 SAP 云平台的连接器。SAP Cloud Connector 2.11.3 之前版本中存在安全漏洞。远程攻击者可利用该漏洞执行注入的代码，进而控制应用程序的运行。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=509151985

3.Google Go 资源管理错误漏洞（CNNVD-201901-883）

Google Go 是美国谷歌（Google）公司的一种针对多处理器系统应用程序的编程进行了优化的编程语言。Google Go 1.10.8 之前版本和 1.11.5 之前的 1.11.x 版本中存在安全漏洞，该漏洞源于程序错误地处理了 P-521 和 P-384 椭圆曲线。攻击者可利用该漏洞造成拒绝服务（CPU 消耗）或可能恢复 ECDH 私钥。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/golang/go/commit/42b42f71cf8f5956c09e66230293dfb5db652360

4. Cisco Small Business RV320 和 RV325 信息泄露漏洞（CNNVD-201901-876）

Cisco Small Business RV320 和 RV325 都是美国思科（Cisco）公司的企业级路由器。使用 1.4.2.15 版本至 1.4.2.19 版本固件的 Cisco Small BusinessRV320 和 RV325 中基于 Web 的管理界面存在信息泄露漏洞，该漏洞源于程序对 URLs 执行了错误的访问控制。远程攻击者可通过 HTTP 或 HTTPS 协议连接受影响的设备并请求 URLs 利用该漏洞检索敏感信息。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-info。

5. CrestronAirMedia AM-100 授权问题漏洞（CNNVD-201901-750）

CrestronAirMedia AM-100 是美国 Crestron Electronics 公司的一款智能家居网关产品。使用 1.6.0.2 之前版本固件的 Crestron AM-100 中的 Web 界面的 return.cgi 脚本存在身份验证绕过漏洞。远程攻击者可利用该漏洞访问管理员功能（例如：配置更新源和重启设备）。

解决措施：目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.crestron.com/

6. Omron CX-Supervisor 命令注入漏洞（CNNVD-201901-738）

Omron CX-Supervisor 是日本欧姆龙（Omron）公司的一款可视化机器控制器。Omron CX-Supervisor 3.42 及之前版本中存在命令注入漏洞。攻击者可借助特制的项目文件利用该漏洞执行程序，创建、写入并读取设备上的文件。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://www.myomron.com/index.php?action=kb&article=1711

7. Cisco SD-WAN Solution 权限许可和访问控制漏洞（CNNVD-201901-868）

Cisco vBond Orchestrator Software 等都是美国思科（Cisco）公司的产品。Cisco vBond Orchestrator Software 是一套安全网络扩展管理软件。vEdge 100 Series Routers 是一款 100 系列的路由器产品。SD-WAN Solution 是运行在其中的一套网络扩展解决方案。Cisco SD-WAN Solution 18.4.0 之前版本中的用户组群配置存在提权漏洞，该漏洞源于程序没有正确地验证参数。远程攻击者可通过向用户组群配置所在的底层操作系统的目录写入特制的文件利用该漏洞获取 root 级别的权限并控制设备。以下产品受到影响：

- Cisco vBond Orchestrator Software
- CiscovEdge 100 Series Routers
- CiscovEdge 1000 Series Routers
- CiscovEdge 2000 Series Routers
- CiscovEdge 5000 Series Routers
- CiscovEdge Cloud Router Platform
- CiscovManage Network Management Software
- CiscovSmart Controller Software

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-sol-escal

8. Microsoft Edge 和 ChakraCore 缓冲区错误漏洞（CNNVD-201901-153）

Microsoft Windows 10 和 Windows Server 2019 都是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2019 是一套服务器操作系统。Edge 是其中的一款 Web 浏览器。ChakraCore 是使用在 Edge 中的一个开源的 Chakra JavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。Microsoft Edge 和 ChakraCore 中存在远程代码执行漏洞。远程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，损坏内存。以下系统版本受到影响：

- MicrosoftWindows 10 版本 1803
- MicrosoftWindows 10 版本 1809
- MicrosoftWindows Server 2019

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0568。

9. Cisco SD-WAN Solution vContainer 访问控制错误漏洞（CNNVD-201901-871）

Cisco SD-WAN Solution 是美国思科（Cisco）公司的一套网络扩展解决方案。vContainer 是其中的一个容器组件。Cisco SD-WAN Solution 18.4.0 之前版本中的 vContainer 存在访问控制错误漏洞，该漏洞源于不安全的默认配置。攻击者可利用该漏洞检索并修改重要的系统文件。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-unaccess

10. MailEnable 路径遍历漏洞（CNNVD-201901-604）

MailEnable 是澳大利亚 MailEnable 公司的一套 POP3 和 SMTP 邮件服务器。MailEnable 8.60 之前版本存在目录遍历漏洞，该漏洞源于程序错误地处理了‘/../’和‘/.. /’序列。攻击者可利用该漏洞读取用户信息，上传文件并删除文件。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.mailenable.com/Standard-ReleaseNotes.txt。

11. ABB CP400PB TextEditor 输入验证漏洞（CNNVD-201901-741）

ABB CP400PB 是瑞士 ABB 公司的一套人机界面编程软件。TextEditor 是其中的一个文本编辑器。ABB CP400PB 2.0.7.05 及之前版本中的 TextEditor 2.0 版本的文件解析器存在输入验证漏洞，该漏洞源于程序没有阻止恶意文件的插入。攻击者可利用该漏洞执行任意代码并造成拒绝服务。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接: https://new.abb.com/products/ABB1SAP500400R0001

12.XytronixResearch&DesignControlByWeb X-320M 跨站脚本漏洞（CNNVD-201901-743）

XytronixResearch&DesignControlByWeb X-320M 是美国 XytronixResearch&Design 公司的一款支持网络的气象站控制器。该产品支持以远程方式查看当前的风速、风向、降水、温度、湿度、太阳辐射和气压等。XytronixResearch&DesignControlByWeb X-320M 中存在跨站脚本漏洞，该漏洞源于程序没有正确地验证输入。远程攻击者可利用该漏洞执行代码。

解决措施：目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.controlbyweb.com/

13.多款 Qualcomm snapdragon 产品竞争条件漏洞（CNNVD-201901-756）

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司应用于不同平台的中央处理器（CPU）产品。多款 Qualcomm snapdragon 产品中存在竞争条件漏洞。攻击者可利用该漏洞造成越边界访问。以下产品（用于移动和可穿戴设备）受到影响：

- Qualcomm MDM9206
- QualcommMDM9607
- QualcommSD 210
- QualcommSD 212
- QualcommSD 205

- QualcommSD 427
- QualcommSD 435
- QualcommSD 450
- QualcommSD 625
- QualcommSD 636
- QualcommSD 835
- QualcommSDA660
- QualcommSDM630
- QualcommSDM660
- QualcommSnapdragon_High_Med_2016

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.qualcomm.com/company/product-security/bulletins

14.Phoenix Contact FL SWITCH 跨站请求伪造漏洞（CNNVD-201901-894）

Phoenix Contact FL SWITCH 是德国菲尼克斯电气（Phoenix Contact）集团的一款工业级以太网交换机。Phoenix Contact FL SWITCH 3xxx 1.35 之前版本、4xxx 1.35 之前版本和 48xx 1.35 之前版本中存在跨站请求伪造漏洞。远程攻击者可利用该漏洞造成 Web 浏览器传递非预期的命令。

解决措施：目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.phoenixcontact.com

2. 接报漏洞情况

本月接报漏洞共计 5664 个，其中信息技术产品漏洞（通用型漏洞）65 个，网络信息系统漏洞（事件型漏洞）5599 个。

表 7　2019 年 1 月漏洞接报情况

序号	报送单位	漏洞总量	通用型漏洞	事件型漏洞
1	上海斗象信息科技有限公司	3293	0	3293
2	网神信息技术（北京）股份有限公司	1646	0	1646
3	中新网络信息安全股份有限公司	304	8	296
4	四川虹微技术有限公司	126	0	126
5	北京数字观星科技有限公司	97	0	97
6	内蒙古奥创科技有限公司	57	9	48
7	北京圣博润高新技术股份有限公司	38	0	38
8	国发中新（北京）科技发展有限公司	24	0	24
9	河南听潮盛世信息技术有限公司	20	4	16
10	西安交大捷普网络科技有限公司	16	6	10
11	广州锦行网络科技有限公司	6	3	3
12	上海三零卫士信息安全有限公司	4	4	0
13	北京安信天行科技有限公司	3	3	0
14	北京江南天安科技有限公司	3	3	0
15	北京启明星辰信息安全技术有限公司	5	5	0
16	北京天融信网络安全技术有限公司	3	3	0

17	北京威努特技术有限公司	3	3	0
18	安徽锋刃信息科技有限公司	2	2	0
19	安天科技股份有限公司	2	2	0
20	北京安华金和科技有限公司	2	2	0
21	东软集团股份有限公司	2	2	0
22	国防科技大学电子对抗学院	2	2	0
23	哈尔滨安天科技集团股份有限公司	2	2	0
24	亚信科技（成都）有限公司	2	2	0
25	杭州迪普科技	1	1	0
26	个人报送	1	1	0
报送总计		5664	65	5599

3. 重大漏洞预警

3.1. 关于 ThinkPHP5.0 远程代码执行漏洞(CNNVD-201901-445)的通报

本月 CNNVD 收到关于 ThinkPHP 5.0 远程代码执行漏洞（CNNVD-201901-445）情况的报送。成功利用此漏洞的攻击者可以对目标系统进行远程代码执行攻击。ThinkPHP 5.0.x - 5.0.23 等多个版本均受此漏洞影响。目前，该漏洞的漏洞验证代码已经公开，同时 ThinkPHP 官方已经发布了该漏洞的修补措施，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

ThinkPHP 是一个免费开源的，快速简单的面向对象的轻量级 PHP 开发框架。该框架常被用来进行二次开发，国内应用非常广泛。Thinkphp 在实现框架中的核心类 Request 的 method 方法实现了表单请求伪装。但由于对 $_POST['_method']属性校验不严格，导致攻击者可以通过变量覆盖掉 Request 类的属性并结合框架特性实现对任意函数的调用，从而实现远程代码执行。

漏洞危害

成功利用此漏洞的攻击者可以对目标系统进行远程代码执行攻击。目前，该漏洞的漏洞验证代码已在互联网上公开，近期被利用的可能性较大。受漏洞影响版本如下：

ThinkPHP 5.0.x - 5.0.23

修复措施

目前，ThinkPHP 官方已经发布更新修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

http://www.thinkphp.cn/down.html

3.2. 关于微软多个安全漏洞

本月，微软官方发布了多个安全漏洞的公告，包括 MicrosoftWindows 权限提升漏洞（CNNVD-201901-176、CVE-2019-0543）、Windows 内核信息泄漏漏洞（CNNVD-201901-137、CVE-2019-0536）、Microsoft Word 远程代码执行漏洞（CNNVD-201901-147、CVE-2019-0585）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，采取修补措施。

漏洞简介

本次漏洞公告涉及 Microsoft Windows 系统、Microsoft Office、Microsoft Word、Microsoft Outlook 、Windows Jet 数据库、Chakra 脚本引擎、Windows Hyper-V 、Windows DHCP 客户端等 Windows 平台下应用软件和组件。漏洞详情如下：

1、 Microsoft Windows 权限提升漏洞（CNNVD-201901-176、CVE-2019-0543）

漏洞简介：当 Windows 内核无法正确处理内存中的对象时，可能就会触发该漏洞。攻击者首先必须登录到系统。然后运行一个经特殊设计的应用程序，才能利用此漏洞。成功利用漏洞的攻击者可以在内核模式中运行任意代码。攻击者可任意安装程序、查看、更改或删除数据、或者创建新帐户等。

2、 Windows 内核信息泄漏漏洞（CNNVD-201901-137、CVE-2019-0536）

漏洞简介：当 Windows 内核不正确地处理内存中的对象时会触发该漏洞。成功利用此漏洞的攻击者可以获取内核信息，从而进一步入侵用户系统。已经过身份验证的攻击者可以通过运行经特殊设计的应用程序来利用此漏洞。

3、Microsoft Word 远程代码执行漏洞（CNNVD-201901-147、CVE-2019-0585）

漏洞简介：当 Microsoft Word 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Word 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。

4、 Microsoft Word 信息泄漏漏洞（ CNNVD-201901-159、CVE-2019-0561）

漏洞简介：当未正确使用 Microsoft Word 宏按钮时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可以从目标系统中读取任意文件。

5、 Microsoft Office 信息泄漏漏洞（CNNVD-201901-160、CVE-2019-0560）

漏洞简介：当 Microsoft Office 不正确地处理内存中的数据时，存在信息泄漏漏洞。攻击者通过设计一个特殊构造的文档诱使用户将其打开，从而获取用户计算机中存储的数据。

6、 Microsoft Outlook 信息泄漏漏洞（CNNVD-201901-161 、CVE-2019-0559）

漏洞简介：当 Microsoft Outlook 不正确地处理特定类型的邮件时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可能会收集用户相关的信息。攻击者通过向用户发送经特殊设计的电子邮件来利用此漏洞，最终获得用户信息。

7、Windows Jet 数据库引擎远程代码执行漏洞（CNNVD-201901-179、CVE-2019-0538）

漏洞简介：当 Windows Jet 数据库引擎不正确地处理内存中的对象时，会触发远程代码执行漏洞。攻击者可以通过诱使用户打开经特殊设计的文件来利用此漏洞。成功利用此漏洞的攻击者可以在用户系统上执行任意代码。

8、Chakra 脚本引擎安全漏洞（CNNVD-201901-178、CVE-2019-0539）、（CNNVD-201901-154、CVE-2019-0567）、（CNNVD-201901-153、CVE-2019-0568）

漏洞简介：Chakra 脚本引擎在 Microsoft Edge 中处理内存中的对象的时可能触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理权限登录，攻击者便可以任意安装程序、查看、更改或删除数据。

9、Windows DHCP 客户端远程代码执行漏洞（CNNVD-201901-173、CVE-2019-0547）

漏洞简介：当攻击者向 Windows DHCP 客户端发送经特殊设计的 DHCP 响应时，会触发该漏洞。成功利用此漏洞的攻击者可以在客户端计算机上运行任意代码。

10、Windows Hyper-V 远程代码执行漏洞（CNNVD-201901-170、CVE-2019-0550）

漏洞简介：当服务器上的 Windows Hyper-V 无法正确验证用户操作系统上经身份验证的用户的输入时，会触发该漏洞。成功利用此漏洞的攻击者可以执行任意代码

安全建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，采取修补措施。微软官方链接地址如下：

序号	漏洞名称	官方链接
1	Microsoft Windows 权限提升漏洞（ CNNVD-201901-176 、CVE-2019-0543）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0543
2	Windows 内核信息泄漏漏洞（CNNVD-201901-137 、CVE-2019-0536）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0536
3	Microsoft Word 远程代码执行漏洞 （ CNNVD-201901-147 、CVE-2019-0585）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0585
4	Microsoft Word 信息泄漏漏洞（CNNVD-201901-159 、CVE-2019-0561）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0561
5	Microsoft Office 信息泄漏漏洞（ CNNVD-201901-160 、CVE-2019-0560）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0560
6	Microsoft Outlook 信息泄漏漏洞（ CNNVD-201901-161 、CVE-2019-0559）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0559
7	Windows Jet 数据库引擎远程代码执行漏洞（CNNVD-201901-179 、CVE-2019-0538）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0538
8	Chakra 脚本引擎安全漏洞（CNNVD-201901-178、CVE-2019-0539）、（CNNVD-201901-154、CVE-2019-0567）、（CNNVD-201901-153、CVE-2019-0568）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0539 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0567

		https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0568
9	Windows DHCP 客户端远程代码执行漏洞（CNNVD-201901-173、CVE-2019-0547）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0547
10	Windows Hyper-V 远程代码执行漏洞（CNNVD-201901-170、CVE-2019-0550）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0550