北京师范大学网络信息安全通告

2019 年 3 月报告

北京师范大学信息网络中心

2019 年 4 月

目录

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2019 年 3 月份采集安全漏洞共 1360 个。本月接报漏洞共计 4650 个，其中信息技术产品漏洞（通用型漏洞）106 个，网络信息系统漏洞（事件型漏洞）4544 个。

重大漏洞预警

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 Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377 、CVE-2019-0784 ）、Internet Explorer 内存损坏漏洞（CNNVD-201903-435、CVE-2019-0763）、Chakra 脚本引擎内存损坏漏洞（CNNVD-201903-421、CVE-2019-0592）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、获取用户数据。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 3 月份新增安全漏洞共 1360 个，从厂商分布来看，Insteon 公司产品的漏洞数量最多，共发布 85 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 9.94%。本月新增漏洞中，超危漏洞 111 个、高危漏洞 392 个、中危漏洞 302 个、低危漏洞 9 个，暂未分级漏洞 546 个。相应修复率分别为 62.16%、51.53%、63.58%、100.00%以及 84.80%。合计 935 个漏洞已有修复补丁发布，本月整体修复率 68.75%。截至 2019 年 3 月 31 日，CNNVD 采集漏洞总量已达 123801 个。

1.1. 漏洞增长概况

2019 年 3 月新增安全漏洞 1360 个，与上月（1038 个）相比增加了 31.10%。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 1271 个。

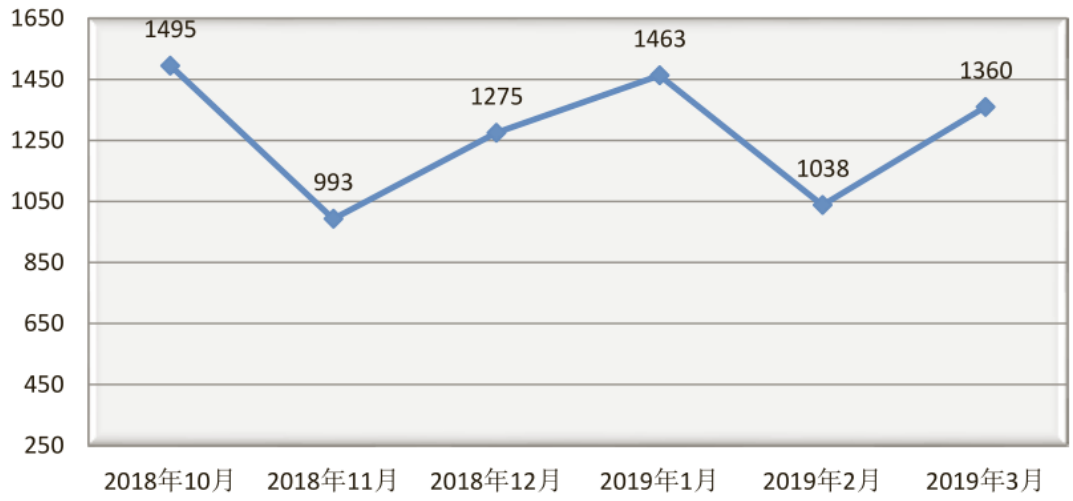

图 1 2018 年 10 月至 2019 年 3 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

3 月厂商漏洞数量分布情况如表 1 所示，Insteon 公司达到 85 个，占本月漏洞总量的 6.25%。本月思科、谷歌等公司的漏洞数量均有所上升，微软的漏洞数量出现较不同程度的下降。

表1 2019 年 3 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	Insteon	85	6.25%
2	Apple	66	4.85%
3	IBM	65	4.78%
4	微软	65	4.78%
5	思科	65	4.78%
6	谷歌	50	3.68%
7	Intel	40	2.94%
8	PHP Scripts Mall	24	1.76%
9	Mozilla	23	1.69%
10	Apache	13	0.96%

1.2.2. 漏洞产品分布

3 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 35 条，其中桌面操作系统 35 条，服务器操作系统 29 条。本月 Apple iOS 漏洞数量最多，共 50 个，占主流操作系统漏洞总量的 16.84%，排名第一。

表 2 2019 年 3 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	50
2	Android	34
3	Apple macOS Mojave	34
4	Windows 10	32
5	Microsoft Windows Sever 1709	25
6	Windows Server 2016	22
7	Windows 7	21
8	Windows Server 2008	20
9	Windows 8.1	19
10	Windows Server 2012	18
11	Windows Rt 8.1	16
12	Linux Kernel	6

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

3 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 9.94%。

表3　2019 年 3 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	162	9.94%
2	缓冲区错误	127	7.79%

3	输入验证	101	6.20%
4	权限许可和访问控制	77	4.72%
5	信息泄露	55	3.37%
6	路径遍历	41	2.52%
7	访问控制错误	30	1.84%
8	SQL 注入	28	1.72%
9	命令注入	27	1.66%
10	跨站请求伪造	26	1.60%
11	信任管理	17	1.04%
12	安全特征问题	17	1.04%
13	代码注入	16	0.98%
14	竞争条件	9	0.55%
15	注入	9	0.55%
16	资源管理错误	9	0.55%
17	数字错误	8	0.49%
18	授权问题	8	0.49%
19	操作系统命令注入	7	0.43%
20	后置链接	2	0.12%
21	配置错误	2	0.12%
22	加密问题	2	0.12%
23	格式化字符串	1	0.06%

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。3 月漏洞危害等级分布如图 2 所示，其中超危漏洞 111 条，占本月漏洞总数的 8.16%。

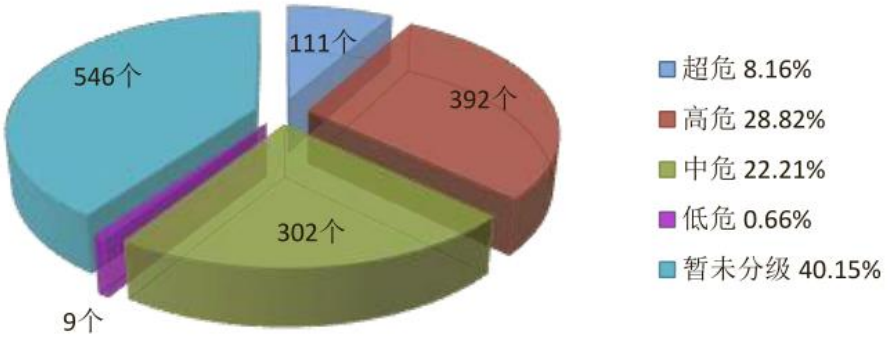

图 2　2019 年 3 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

3 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Cisco、Google、Microsoft 等十个厂商共 496 条漏洞，占本月漏洞总数的 36.47%，漏洞修复率为 77.22%，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 Apple、IBM、Google、Mozilla、Apache 等公司本月漏洞修复率均为 100%，共 334 条漏洞已全部修复。

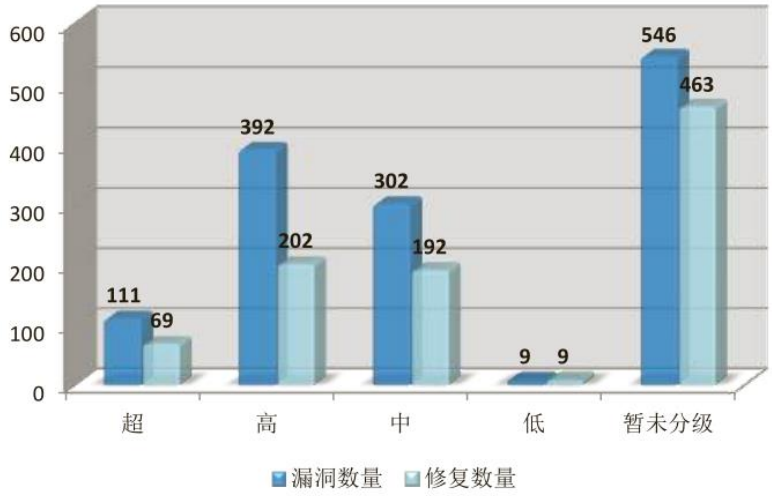

图 3　2019 年 3 月漏洞修复数量统计

1.3.2. 厂商修复情况

3 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Cisco、Google、Microsoft 等十个厂商共 496 条漏洞，占本月漏洞总数的 36.47%，漏洞修复率

为 77.22%，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 Apple、IBM、Google、Mozilla、Apache 等公司本月漏洞修复率均为 100%，共 334 条漏洞已全部修复。

表 4 2019 年 3 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	Insteon	85	0	0.00%
2	Apple	66	66	100.00%
3	IBM	65	65	100.00%
4	Microsoft	65	6 4	98.46%
5	Cisco	65	64	98.46%
6	Google	50	50	100.00%
7	Intel	40	38	95.00%
8	PHP Scripts Mall	24	0	0.00%
9	Mozilla	23	23	100.00%
10	Apache	13	13	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 111 个，其中重要漏洞实例如表 5 所示。

表 5 2019 年 3 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	信息泄露	CNNVD-201903-489	华为	Huawei OceanStor UDS 信息泄露漏洞（CNNVD-201903-489）
2	信任管理	CNNVD-201903-591	Cobham	Cobham Satcom Sailor 250 和Cobham Satcom Sailor 500 信任管理漏洞（CNNVD-201903-591）

3	输入验证	CNNVD-201903-902	Micro Focus	Micro Focus ArcSight Logger输入验证漏洞（ CNNVD-201903-902 ）
		CNNVD-201703-1372	Fortinet	
4	授权问题	CNNVD-201903-645	Columbia Weather Systems	Columbia Weather Systems Weather MicroServer 授权问题漏洞（CNNVD-201903-645）
5	权限许可和访问控制	CNNVD-201903-496	Cisco	Cisco Common Services Platform Collector 权限许可和访问控制漏洞（CNNVD-201903-496）
		CNNVD-201903-018	SolarWinds	
6	命令注入	CNNVD-201902-1035	Elasticsearch	Elasticsearch Kibana 命令注入漏洞（CNNVD-201902-1035）
		CNNVD-201902-1037		
7	路径遍历	CNNVD-201903-909	Atlassian	Atlassian Confluence Server 路径遍历漏洞（CNNVD-201903-909）
8	缓冲区错误	CNNVD-201903-091	Rockwell Automation	Rockwell Automation RSLinx Classic 缓冲区错误漏洞（CNNVD-201903-091）
		CNNVD-201902-988	Cisco	
9	访问控制错误	CNNVD-201903-604	Five9	Five9 Agent Desktop Plus 访问控制错误漏洞（CNNVD-201903-604）
		CNNVD-201903-043	Druide informatique	
10	代码注入	CNNVD-201903-642	Columbia Weather Systems	Columbia Weather SystemsWeather MicroServer 代码注入漏洞（CNNVD-201903-642）
11	安全特征问题	CNNVD-201903-303 CNNVD-201903-300 CNNVD-201903-299 CNNVD-201903-298 CNNVD-201903-296	CloudBees	CloudBees Jenkins Job DSL Plugin 安全特征问题漏洞（CNNVD-201903-303）

1. Huawei OceanStor UDS 信息泄露漏洞(CNNVD-201903-489)

Huawei OceanStor UDS 是中国华为（Huawei）公司的一套基于 ARM 架构的高密度存储节点及分布式存储系统。Huawei OceanStor UDS V100R002C01SPC101 及之前版本中存在信息泄露漏洞。远程攻击者可通过截获和修改加载信息利用该漏洞破坏设备的目录文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.huawei.com/en/psirt/security-advisories/hw-417839

2. Cobham Satcom Sailor 250 和 Cobham Satcom Sailor 500 信任管理漏洞(CNNVD-201903-591)

Cobham Satcom Sailor 250 和 Cobham Satcom Sailor 500 都是英国 Cobham 公司的一款船载海事卫星宽带终端设备。使用 1.25 之前版本固件的 Cobham Satcom Sailor 250 和 500 中存在安全漏洞。远程攻击者可利用该漏洞无需用户密码便可更改任意用户的账户密码（包括默认的‘admin’账户）。目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://www.cobham.com/

3. Micro Focus ArcSight Logger 输入验证漏洞（CNNVD-201903-902）

Micro Focus ArcSight Logger 是英国 Micro Focus 公司的一套日志管理软件。该软件能够收集并整合来自任何日志生成来源的数据，用于日志管理、搜索、编制索引、报告、分析和保留。Micro Focus ArcSight Logger 6.7 之前版本中存在输入验证漏洞。远程攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://softwaresupport.softwaregrp.com/doc/KM03355866

4. Columbia Weather Systems Weather MicroServer 授权问题漏洞（CNNVD-201903-645）

Columbia Weather Systems Weather MicroServer 是美国 Columbia Weather Systems 公司的一款气象监测设备。Columbia Weather Systems

Weather MicroServer MS_2.6.9900 及之前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，操纵设备并造成拒绝服务。

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://columbiaweather.com/

5. Cisco Common Services Platform Collector 权限许可和访问控制漏洞（CNNVD-201903-496）

Cisco Common Services Platform Collector（CSPC）是美国思科（Cisco）公司的一款通用服务平台数据收集器。该产品通过轮询思科设备的基本库存和配置数据分析网络性能，并识别风险和漏洞。Cisco CSPC 2.7.2 版本至 2.7.4.5 版本和 2.8.1.2 之前的 2.8.x 版本中存在权限许可和访问控制漏洞，该漏洞源于该软件所带有的用户账户使用了默认的静态密码。远程攻击者可利用该漏洞登录到 CSPC 中。

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-20190313-cspcscv

6. Elasticsearch Kibana Elasticsearch Kibana 命令注入漏洞（CNNVD-201902-1035）

Elasticsearch Kibana 是荷兰 Elasticsearch 公司的一套开源的、基于浏览器的分析和搜索 Elasticsearch 仪表板工具。Elasticsearch Kibana 5.6.15 之前版本和 6.6.1 之前版本中的 Timelion visualizer 存在安全漏洞。远程攻击者可通过发送请求利用该漏洞执行 JavaScript 代码并可能以 Kibana 进程权限执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.elastic.co/cn/community/security

7. Atlassian Confluence Server 路径遍历漏洞（CNNVD-201903-909）

Atlassian Confluence Server 是澳大利亚 Atlassian 公司的一套专业的企业知识管理与协同软件，也可以用于构建企业 WiKi。Atlassian Confluence Server 中存在安全漏洞。远程攻击者可利用该漏洞执行代码。以下版本受到影响：

- Atlassian Confluence Server 6.6.12 之前版本
- Atlassian Confluence Server 6.7.0 版本至 6.12.3 之前版本
- Atlassian Confluence Server 6.13.0 版本至 6.13.3 之前版本
- Atlassian Confluence Server 6.14.0 版本至 6.14.2 之前版本

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://jira.atlassian.com/browse/CONFSERVER-57974

8. Rockwell Automation RSLinx Classic 缓冲区错误漏洞（CNNVD-201903-091）

Rockwell Automation RSLinx Classic 是美国罗克韦尔（RockwellAutomation）公司的一套工厂通信解决方案。该方案支持通过 Allen-Bradley 可编程控制器访问 RockwellSoftware 和 Allen-Bradley 应用程序等。Rockwell Automation RSLinx Classic 4.10.00 及之前版本中的.dll 文件存在基于栈的缓冲区溢出漏洞。远程攻击者可利用该漏洞在目标设备上执行代码。

目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：
https://www.rockwellautomation.com

9. Five9 Agent Desktop Plus 访问控制错误漏洞（CNNVD-201903-604）

Five9 Agent Desktop Plus 是美国 Five9 公司的一套基于云的联络中心软件。Five9 Agent Desktop Plus 10.0.70 版本中存在访问控制错误漏洞。远程攻击者可利用该漏洞执行代码。

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.five9.com/

10. Columbia Weather Systems Weather MicroServer 代码注入漏洞（CNNVD-201903-642）

Columbia Weather Systems Weather MicroServer 是美国 Columbia Weather Systems 公司的一款气象监测设备。Columbia Weather Systems Weather MicroServer MS_2.6.9900 及之前版本中存在代码注入漏洞。远程攻击者可利用该漏洞执行代码。

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://columbiaweather.com/

11. CloudBees Jenkins Job DSL Plugin 安全特征问题漏洞（CNNVD-201903-303）

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。Job DSL Plugin 是使用在其中的一个支持 DSL 以编程方式创建项目的插件。CloudBees Jenkins Job DSL Plugin 1.71 及之前版本中存在安全特征问题漏洞。攻击者可利用该漏洞绕过沙盒保护，在 Jenkinsmaster 上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1342

1.4.2. 高危漏洞实例

本月高危漏洞共 392 个，其中重点漏洞实例如表 6 所示。

表 6 2019 年 3 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	资源管理错误	CNNVD-201903-247	ImageMagick Studio	ImageMagick Studio ImageMagick 资源管理错误漏洞（CNNVD-
		CNNVD-201903-188	Cisco	

		CNNVD-201903-495		201903-247）
2	注入	CNNVD-201903-263	Google	Google Go 注入漏洞（CNNVD-201903-263）
3	信息泄露	CNNVD-201902-978	NetApp	NetApp Clustered Data ONTAP 信息泄露漏洞（CNNVD-201902-978）
		CNNVD-201903-837	IBM	
4	信任管理	CNNVD-201903-612	Threshold	Threshold eVisitorPass 信任管理漏洞（CNNVD-201903-612）
		CNNVD-201903-498	Dell	
		CNNVD-201903-308 CNNVD-201903-310	CloudBees	
5	输入验证	CNNVD-201903-189 CNNVD-201903-175 CNNVD-201903-172	Cisco	Apache Qpid Broker-J 输入验证漏洞（CNNVD-201903-033）
		CNNVD-201903-033	Apache	
6	权限许可和访问控制	CNNVD-201903-545 CNNVD-201903-565	Intel	Intel Graphics Driver forWindows 权限许可和访问控制漏洞（CNNVD-201903-545）
		CNNVD-201903-485	IBM	
7	配置错误	CNNVD-201903-1116	Cisco	Cisco IOS XE配置错误漏洞 （CNNVD-201903-1116 ）
		CNNVD-201903-167		
8	命令注入	CNNVD-201903-427	F5	Atlassian Sourcetree 命令注入漏洞（CNNVD-201903-268）
		CNNVD-201903-154 CNNVD-201903-165 CNNVD-201903-171	Cisco	
		CNNVD-201903-267 CNNVD-201903-268	Atlassian	
9	路径遍历	CNNVD-201903-719	Wowza Media Systems	Cisco IP Phone 8800 Series Session InitiationProtocol 软件路径遍历漏洞（CNNVD-201903-69）
		CNNVD-201903-696	Cisco	

10	跨站请求伪造	CNNVD-201903-688	Cisco	Cisco IP Phone 8800 Series Series Session Initiation Protocol 软件跨站请求伪造漏洞（CNNVD-201903-688）
11	跨站脚本	CNNVD-201903-654 CNNVD-201903-632	Columbia Weather Systems	Columbia Weather Systems Weather MicroServer 跨站脚本漏洞（CNNVD-201903-654）
12	竞争条件	CNNVD-201903-588	CapMon	CapMon Access Manager 竞争条件（CNNVD-201903-588）
13	缓冲区错误	CNNVD-201903-575	LCDS	LCDS LAquis SCADA 缓冲区错误漏洞（CNNVD-201903-575）
		CNNVD-201903-548 CNNVD-201903-546	Intel	
		CNNVD-201903-289 CNNVD-201903-285	IBM	
14	后置链接	CNNVD-201902-1004	McAfee	McAfee Endpoint Security 后置链接漏洞（CNNVD-201902-100）
15	访问控制错误	CNNVD-201903-200	中天网络科技	HID Global EasyLobby Solo 访问控制错误漏洞（CNNVD-201903-614）
		CNNVD-201903-614 CNNVD-201903-615	HID Global	
16	代码注入	CNNVD-201903-506	OTRS	Open Ticket Request System 代码注入漏洞（CNNVD-201903-506）

1、ImageMagick Studio ImageMagick 资源管理错误漏洞（CNNVD-201903-247）

ImageMagick Studio ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图像处理软件。该软件可读取、转换或写入多种格式的图片。ImageMagick 7.0.8-25 之前版本中的 coders/pcd.c 文件存在资源管理错误漏洞。攻击者可利用该漏洞造成拒绝服务。

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/ImageMagick/ImageMagick/commit/1e6a3ace073c9ec9c71e439c111d23c6e66cb6ae

2、Google Go 注入漏洞 （CNNVD-201903-263）

Google Go 是美国谷歌（Google）公司的一款静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。基于 Windows 平台的 Google Go 1.12 及之前版本中存在注入漏洞，该漏洞源于程序错误地使用了 LoadLibrary 功能。攻击者可利用该漏洞注入 DLL。

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/issues/306420

3、NetApp Clustered Data ONTAP NetApp Clustered Data ONTAP 信息泄露漏洞（CNNVD-201902-978）

NetApp Clustered Data ONTAP 是美国 NetApp 公司的一套用于集群模式的存储操作系统。NetApp Clustered Data ONTAP 9.1P15 之前版本和 9.3P7 之前的 9.3 版本中存在信息泄露漏洞。攻击者可利用该漏洞泄露敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://security.netapp.com/advisory/ntap-20190227-0001/

4、Threshold eVisitorPass 信任管理漏洞（CNNVD-201903-612）

Threshold eVisitorPass 是加拿大 Threshold 公司的一套访客管理系统。Threshold eVisitorPass 1.5.5.2 版本中存在信任管理漏洞，该漏洞源于程序使用了默认的管理凭证。本地攻击者可利用该漏洞获取该系统的全部访问权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
http://support.evisitorpass.com/Release_Notes.html

5、Apache Qpid Broker Apache Qpid Broker-J 输入验证漏洞（CNNVD-201903-033）

Apache Qpid 是美国阿帕奇（Apache）软件基金会的一款面向对象的消息中间件。该产品是一个 AMQP（高级消息队列协议）的实现，可以和符合 AMQP 协议的系统进行通信，并提供了 C++、Python、Java、C#等编程语言的客户端库。Qpid Broker-J 是其中的一个使用 Java 编写的中间件消息代理组件。Apache Qpid Broker-J 6.0.0 版本至 7.0.6 版本和 7.1.0 版本中存在输入验证漏洞。攻击者可通过发送的特制命令利用该漏洞造成代理实例崩溃。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://issues.apache.org/jira/browse/QPID-8273

6、Intel Graphics Driver for Windows Intel Graphics Driver for Windows 权限许可和访问控制漏洞（CNNVD-201903-545）

Intel Graphics Driver for Windows 是美国英特尔（Intel）公司的一款适用于 Windows 平台的显卡驱动程序。Kernel Mode Driver 是其中的一个内核模式驱动程序。基于 Windows 平台的 Intel Graphics Driver 中的 Kernel Mode Driver 存在权限许可和访问控制漏洞。本地攻击者可利用该漏洞执行任意代码。以下版本受到影响：

- Intel Graphics Driver 10.18.x.5059 之前版本
- Intel Graphics Driver 10.18.x.5057 之前版本
- Intel Graphics Driver 20.19.x.5063 之前版本
- Intel Graphics Driver 21.20.x.5064 之前版本
- Intel Graphics Driver 24.20.100.6373 之前版本

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00189.html

7、Cisco IOS XE Cisco IOS XE 配置错误漏洞（CNNVD-201903-1116）

Cisco IOS XE 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。Cisco IOS XE 中的 Web UI 存在配置错误漏洞,该漏洞源于程序没有对 Web UI 中的文件执行正确的访问控制。当设备启用了 Web 服务器功能时，远程攻击者可通过发送恶意的请求利用该漏洞访问敏感的配置信息。

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-20190327-xeid

8、Atlassian Sourcetree Atlassian Sourcetree 命令注入漏洞（CNNVD-201903-268）

Atlassian Sourcetree 是澳大利亚 Atlassian 公司的一款免费的 Git 和 Mercurial 客户端工具，它能够利用可视化界面管理存储库。基于 Windows 平台的 Atlassian Sourcetree 0.5a 版本至 3.0.15 之前版本中存在命令注入漏洞。远程攻击者可利用该漏洞在系统上执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://jira.atlassian.com/browse/SRCTREEWIN-11289

9、Cisco IP Phone 8800 Series l Session Initiation Protocol 软件路径遍历漏洞（CNNVD-201903-696）

Cisco IP Phone 8800 Series 是美国思科（Cisco）公司的一款 8800 系列的 IP 电话。Session Initiation Protocol（SIP）Software 是其中的一款会话发起协议软件。Cisco IP Phone 8800 Series 中的 SIP 软件存在路径遍

历漏洞。远程攻击者可通过上传无效的文件利用该漏洞在文件系统上的任意地址写入文件。以下产品受到影响：

- Cisco Wireless IP Phone 8821-EX（SIP 软件 11.0(5)版本）
- Cisco IP Conference Phone 8832（SIP 软件 12.5(1)SR1 版本）
- 其他 Cisco IP Phone 8800 系列产品（SIP 软件 12.5(1)SR1 版本）

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-20190320-ipptv

10、Cisco IP Phone 8800 Series Session Initiation Protocol 软件跨站请求伪造漏洞（CNNVD-201903-688）

Cisco IP Phone 8800 Series 是美国思科（Cisco）公司的一款 8800 系列的 IP 电话。Session Initiation Protocol（SIP）Software 是其中的一款会话发起协议软件。Cisco IP Phone 8800 Series 中的 SIP 软件的基于 Web 的管理界面存在跨站请求伪造漏洞，该漏洞源于程序没有执行充分地跨站请求伪造保护。远程攻击者可通过诱使用户访问特制链接利用该漏洞在目标设备上执行任意操作。以下产品受到影响：

- Cisco Wireless IP Phone 8821-EX（SIP 软件 11.0(5)版本）
- Cisco IP Conference Phone 8832（SIP 软件 11.0(5)版本）
- 其他 Cisco IP Phone 8800 系列产品（SIP 软件 12.5(1)SR1 版本）

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-20190320-ip-phone-csrf

11、Columbia Weather Systems Weather MicroServer 跨站脚本漏洞（CNNVD-201903-654）

Columbia Weather Systems Weather MicroServer 是美国 ColumbiaWeather Systems 公司的一款气象监测设备。Columbia Weather Systems Weather MicroServer MS_2.6.9900 及之前版本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任意的 Web 脚本。

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://columbiaweather.com/

12、CapMon Access Manager 竞争条件漏洞 （CNNVD-201903-588）

CapMon Access Manager 是丹麦 CapMon 公司的一套访问管理软件。该软件支持应用程序白名单/黑名单、审计日志等功能。CapMon Access Manager 5.4.1.1005 版本中的 CALRunElevated.exe 文件存在竞争条件漏洞。攻击者可利用该漏洞获取管理员权限。

目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://capmon.dk/

13、LCDS LAquis SCADA 缓冲区错误漏洞（CNNVD-201903-575）

LCDS LAquis SCADA 是巴西 LCDS 公司的一套 SCADA（数据采集与监视控制）系统。该系统主要用于对拥有通信技术的设备进行数据采集和过程控制。LCDS LAquis SCADA 中存在越界写入漏洞。远程攻击者可借助特制的 ELS 文件利用该漏洞在当前进程的上下文中执行代码。

目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://laquisscada.com/

14、McAfee Endpoint Security 后置链接漏洞（CNNVD-201902-100）

McAfee Endpoint Security（ENS）是美国迈克菲（McAfee）公司的一套提供智能协作和先进的威胁防御的框架。该框架支持对实时通信的整个威胁防御

生命周期进行控制并进行可操作的威胁取证等。McAfee ENS 10.6.1 及之前版本中的 Microsoft Windows 客户端存在后置链接漏洞。本地攻击者可利用该漏洞获取提升的权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kc.mcafee.com/corporate/index?page=content&id=SB10254

15、HID Global EasyLobby Solo 访问控制错误漏洞（CNNVD-201903-614）

HID Global EasyLobby Solo 是美国 HID Global 公司的一套安全访客管理（SVM）软件。HID Global EasyLobby Solo 11.0.4563 版本中存在访问控制错误漏洞。本地攻击者可利用该漏洞在电脑上执行未授权的操作。

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.hidglobal.com/

16、Open Ticket Request System 代码注入漏洞（CNNVD-201903-506）

Open Ticket Request System（OTRS）是德国 OTRS 集团的一套开源缺陷跟踪管理系统软件。该软件将电话，邮件等各种渠道提交进来的服务请求归类为不同的队列、服务级别，服务人员通过 OTRS 系统来跟踪和回复客户。OTRS 5.0.34 之前的 5.x 版本、6.0.16 之前的 6.x 版本和 7.0.4 之前的 7.x 版本中存在代码注入漏洞。攻击者可通过上传特制的资源利用该漏洞执行 JavaScript 代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://community.otrs.com/security-advisory-2019-01-security-update-for-otrs-framework--6

2. 接报漏洞情况

本月接报漏洞共计 4650 个，其中信息技术产品漏洞（通用型漏洞）106 个，网络信息系统漏洞（事件型漏洞）4544 个。

表 7　2019 年 3 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	2040	0	2040
2	网神信息技术（北京）股份有限公司	1909	0	1909
3	中新网络信息安全股份有限公司	282	1	281
4	内蒙古奥创科技有限公司	102	13	89
5	北京数字观星科技有限公司	83	0	83
6	西安四叶草信息技术有限公司	47	7	40
7	北京圣溥润高新技术服份有限公司	40	0	40
8	北京启明星辰信息安全技术有限公司	39	39	0
9	国发中新（北京）科技发展有限公司	24	0	24
10	广州锦行网络科技有限公司	22	3	19
11	匿名	14	14	0
12	杭州安恒信息技术股份有限公司	7	7	0
13	北京天地和兴科技有限公司	6	0	6
14	河南听潮盛世信息技术有限公司	6	0	6
15	西安交大捷普网络科技有限公司	6	5	1

16	个人	5	3	2
17	广州竞远安全技术股份有限公司	3	3	0
18	东方电气启明星辰工控信息安全联合实验室	3	3	0
19	北京安信天行科技有限公司	2	0	2
20	梆梆安全	1	1	0
21	Pockr 安全团队	1	1	0
22	上海大学机电工程与自动化学院	1	1	0
23	山东华鲁科技发展股份有限公司	1	0	1
24	厦门服云信息科技有限公司	1	1	0
25	南宁职业技术学院	1	1	0
26	北京天融信网络安全技术有限公司	1	1	0
27	江苏国瑞信安科技有限公司	1	0	1
28	北京六方领安网络科技有限公司	1	1	0
29	北京威努特技术有限公司	1	1	0
报送总计		4650	106	4544

3. 重大漏洞预警

3.1. 关于微软多个安全漏洞的通报

本月，微软官方发布了多个安全漏洞公告，包括 Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377、CVE-2019-0784）、Internet Explorer 内存损坏漏洞（CNNVD-201903-435、CVE-2019-0763）、Chakra 脚本引擎内存损坏漏洞（CNNVD-201903-421、CVE-2019-0592）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、获取用户数据。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 、ActiveX 插件、Internet Explorer 浏览器、Chakra 脚本引擎、Microsoft XML Core Services 分析器、TFTP 服务器、VBScript 引擎、Windows DHCP 客户端等 Windows 平台下应用软件和组件。漏洞详情如下：

1、Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377、CVE-2019-0784）

漏洞简介：ActiveX 处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可导致攻击者在对象内存中执行任意代码。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用户权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

2、Internet Explorer 内存损坏漏洞 （ CNNVD-201903-435 、CVE-2019-0763）

漏洞简介：：当 Internet Explorer 不正确地访问内存中的对象时会触发该漏洞。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，从而进一步安装程序、查看、更改或删除数据、创建新帐户。

3、Chakra 脚本引擎内存损坏漏洞 （CNNVD-201903-421、CVE-2019-0592）

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。

4、MS XML 远程代码执行漏洞（CNNVD-201903-385、CVE-2019-0756）

漏洞简介：当 Microsoft XML Core Services 分析器处理用户输入时，存在远程代码执行漏洞。攻击者需要诱使用户点击电子邮件或即时消息中的链接以使用户链接到存在恶意代码的网站。当 Internet Explorer 分析 XML 内容时，攻击者可以远程运行恶意代码控制用户的系统。

5、Windows 部署服务 TFTP 服务器远程代码执行漏洞（CNNVD-201903-384、CVE-2019-0603）

漏洞简介：Windows 部署服务 TFTP 服务器在处理内存中的对象时存在远程代码执行漏洞。攻击者可以创建经特殊设计的请求，提升 Windows 权限，从而执行恶意代码。

6、Windows VBScript 引擎远程代码执行漏洞（CNNVD-201903-386、CVE-2019-0666）、（CNNVD-201903-398、CVE-2019-0667）

漏洞简介：VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。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用户权限登录，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。

7、Windows DHCP 客户端远程代码执行漏洞（CNNVD-201903-375、CVE-2019-0697）、（CNNVD-201903-389 、CVE-2019-0698）、（CNNVD-201903-391、CVE-2019-0726）

漏洞简介：当攻击者向 Windows DHCP 服务器发送经特殊设计的 DHCP 数据包时，会触发该漏洞。成功利用此漏洞的攻击者可以在服务器上执行任意代码。

8、Win32k 信息泄漏漏洞（CNNVD-201903-373、CVE-2019-0776）、（CNNVD-201903-452、CVE-2019-0808）

漏洞简介：当 Win32k 组件不正确地提供内核信息时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可以获取用户信息，从而进一步入侵用户系统。要利用此漏洞，攻击者需登录系统，运行专门设计的应用程序，该应用程序可以利用漏洞控制受影响的系统。

9、Microsoft Edge 内存损坏漏洞 （CNNVD-201903-448、CVE-2019-0779）

漏洞简介：当 Microsoft Edge 不正确地访问内存中的对象时会触发该漏洞。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用户权限登录，攻击者便可以控制受影响的系统。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。

修复措施

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	Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377、CVE-2019-0784）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0784
2	Internet Explorer 内存损坏漏洞 （ CNNVD-201903-435 、CVE-2019-0763）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0763
3	Chakra 脚本引擎内存损坏漏洞 （ CNNVD-201903-421 、CVE-2019-0592）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0592
4	MS XML 远程代码执行漏洞（ CNNVD-201903-385 、CVE-2019-0756）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0756
5	Windows 部署服务 TFTP 服务器远程代码执行漏洞（CNNVD-201903-384 、CVE-2019-0603）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0603
6	Windows VBScript 引擎远程代码执行漏洞 （ CNNVD-201903-386 、CVE-2019-0666 ）、（CNNVD-201903-398 、CVE-2019-0667）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0666 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0667

7	Windows DHCP 客户端远程代码执行漏洞（CNNVD-201903-375 、CVE-2019-0697 ）、（CNNVD-201903-389 、CVE-2019-0698）、（CNNVD-201903-391 、CVE-2019-0726）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0697 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0698 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0726
8	Win32k 信息泄漏漏 洞（CNNVD-201903-373 、CVE-2019-0776）、（CNNVD-201903-452、CVE-2019-0808）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0776 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0808
9	Microsoft Edge 内存损坏漏洞（CNNVD-201903-448、CVE-2019-0779）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0779