北京师范大学网络信息安全通告

2019 年 6 月报告

北京师范大学信息网络中心

2019 年 7 月

目录

漏洞态势

1. 公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2019 年 6 月份新增安全漏洞共 1307 个，从厂商分布来看，HPE 公司产品的漏洞数量最多，共发布 98 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 14.15%。本月新增漏洞中，超危漏洞 163 个、高危漏洞 497 个、中危漏洞 540 个、低危漏洞 107 个，相应修复率分别为 69.94%、80.68%、72.41%以及 31.78%。合计 940 个漏洞已有修复补丁发布，本月整体修复率 71.92%。截至 2019 年 6 月 30 日，CNNVD 采集漏洞总量已达 127859 个。

1.1. 漏洞增长概况

2019 年 6 月新增安全漏洞 1307 个，与上月（1285 个）相比增加了 1.71%。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 1310 个。

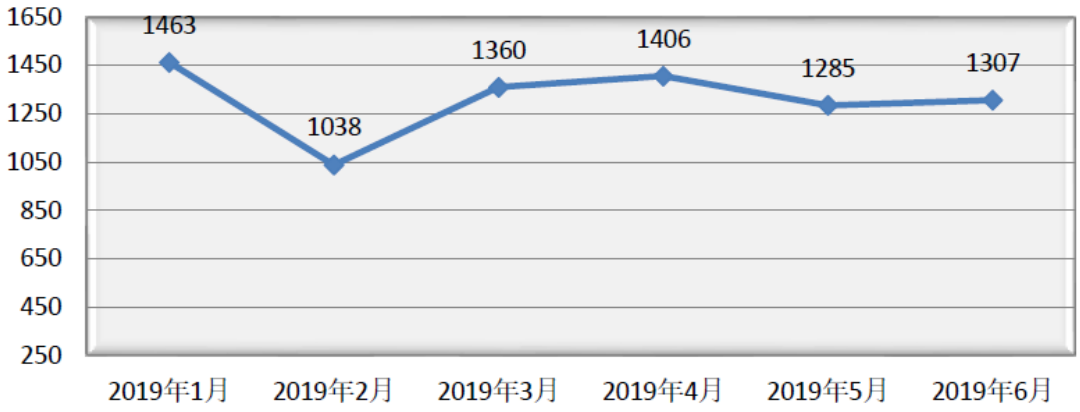

图 1 2019 年 1 月至 2019 年 6 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

6 月厂商漏洞数量分布情况如表 1 所示，HPE 公司达到 98 个，占本月漏洞总量的 7.50%。本月 HPE、微软、IBM 等公司的漏洞数量均有所上升。

表1　2019 年 6 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	HPE	98	7.50%
2	微软	90	6.89%
3	IBM	86	6.58%
4	Magento	61	4.67%
5	思科	39	2.98%
6	谷歌	31	2.37%
7	Intel	26	1.99%
8	Qualcomm	19	1.45%
9	Moxa	14	1.07%
10	Linux	13	0.99%

1.2.2. 漏洞产品分布

6 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 62 条，其中桌面操作系统 62 条，服务器操作系统 62 条。本月 Windows 10 漏洞数量最多，共 50 个，占主流操作系统漏洞总量的 12.95%，排名第一。

表 2　2019 年 5 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	Windows 10	50
2	Windows Server 1803	45
3	Windows Server 1903	42
4	Windows Server 2008	42
5	Windows 7	42
6	Windows Server 2016	39
7	Windows Server 2012	35
8	Windows Rt 8.1	34
9	Windows 8.1	32
10	Linux Kernel	13
11	Android	12

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

6 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 14.15%。

表3　2019 年 6 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	185	14.15%
2	缓冲区错误	132	10.10%
3	输入验证错误	106	8.11%
4	信息泄露	92	7.04%
5	SQL 注入	75	5.74%
6	权限许可和访问控制问题	68	5.20%
7	代码问题	61	4.67%
8	命令注入	57	4.36%
9	访问控制错误	51	3.90%
10	跨站请求伪造	50	3.83%
11	信任管理问题	39	2.98%
12	注入	38	2.91%
13	授权问题	36	2.75%
14	路径遍历	35	2.68%
15	资源管理错误	32	2.45%
16	加密问题	18	1.38%
17	安全特征问题	13	0.99%
18	代码注入	11	0.84%
19	操作系统命令注入	11	0.84%
20	格式化字符串错误	11	0.84%
21	处理逻辑错误	4	0.31%
22	日志信息泄露	3	0.23%
23	数字错误	3	0.23%
24	参数注入	2	0.15%
25	后置链接	2	0.15%
26	数据伪造问题	2	0.15%
27	竞争条件问题	2	0.15%
28	配置错误	1	0.08%

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。6 月漏洞危害等级分布如图 2 所示，其中超危漏洞 163 条，占本月漏洞总数的 12.47%。

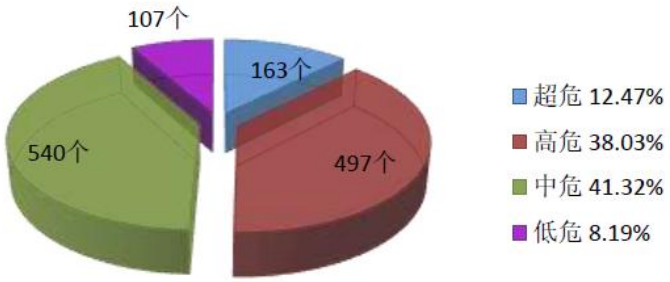

图 2　2019 年 6 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

6 月漏洞修复情况按危害等级进行统计见图 3。其中高危漏洞修复率最高，达到 80.68%，低危漏洞修复率最低，比例为 31.78%。与上月相比，本月中危漏洞修复率有所上升，超危、高危、低危漏洞修复率有所下降。总体来看，本月整体修复率上升，由上月的 72.45%下降至本月的 71.92%。。

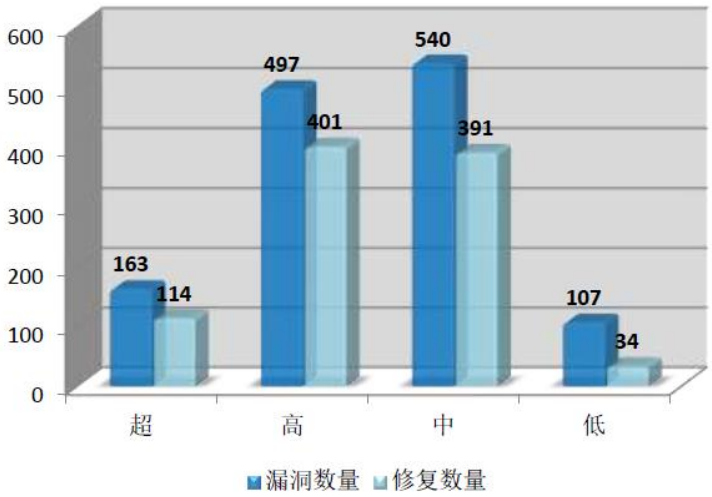

图 3　2019 年 6 月漏洞修复数量统计

1.3.2 厂商修复情况

6 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 HPE、Microsoft、IBM 等十个厂商共 480 条漏洞，占本月漏洞总数的 36.73%，漏洞修复率为 93.75%，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 Adobe、Microsoft、Apple、GitLab 等公司本月漏洞修复率均为 100%，共 392 条漏洞已全部修复。

表 4　2019 年 6 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	HPE	98	98	100.00%
2	Microsoft	90	89	98.89%
3	IBM	86	85	98.84%
4	Magento	64	64	100.00%
5	Cisco	39	38	97.44%
6	Google	31	31	100.00%
7	Intel	26	15	57.69%
8	Qualcomm	19	19	100.00%
9	Moxa	14	0	0.00%
10	Linux	13	11	84.62%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 163 个，其中重要漏洞实例如表 5 所示。

表 5　2019 年 6 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	注入	CNNVD-201906-109	HPE	Magento 注入漏洞

		CNNVD-201906-135		（CNNVD-201906-971）
		CNNVD-201906-971	Magento	
2	信任管理问题	CNNVD-201906-104	Prima Systems	WAGO Industrial Managed Switches 852-303、852-1305 和 852-1505 信任管理问题漏洞（CNNVD-201906-586）
		CNNVD-201906-1072	Sick	
		CNNVD-201906-512	Red Hat	
		CNNVD-201906-558	Fuji Electric	
		CNNVD-201906-586	WAGO	
		CNNVD-201906-591		
		CNNVD-201906-822	华硕	
3	输入验证错误	CNNVD-201906-144	SweetScape Software	Intel RAID Web Console 3 输入验证错误漏洞（CNNVD-201906-575）
		CNNVD-201906-169	HPE	
		CNNVD-201906-206		
		CNNVD-201906-209		
		CNNVD-201906-220		
		CNNVD-201906-261	PaperCut	
		CNNVD-201906-272	Dell	
		CNNVD-201906-575	Intel	
4	授权问题	CNNVD-201906-031	AU Optronics	AU Optronics Solar Data Recorder 授权问题漏洞（CNNVD-201906-031）
		CNNVD-201906-079	Qualcomm	
		CNNVD-201906-211	HPE	
		CNNVD-201906-221		
5	权限许可和访问控制问题	CNNVD-201906-1029	Cisco	Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-201906-1029）
		CNNVD-201906-223	Kromtech Alliance	
		CNNVD-201906-773	WordPress	
6	命令注入	CNNVD-201906-110	HPE	ZTE MF920 命令注入漏洞（CNNVD-201906-371）
		CNNVD-201906-129		
		CNNVD-201906-371	中兴通讯	
		CNNVD-201906-399	友讯	
		CNNVD-201906-400	NETGEAR	
		CNNVD-201906-401	Ubiquiti	
		CNNVD-201906-514	Adobe	
		CNNVD-201906-768	伟易达	
		CNNVD-201906-935	联想	
		CNNVD-201906-940		
7	路径遍历	CNNVD-201906-133	HPE	HPE Intelligent Management Center PLAT 路径遍历漏洞（CNNVD-201906-133）
8	缓冲区	CNNVD-201906-075	Qualcomm	Advantech WebAccess/SCADA

	错误	CNNVD-201906-1075	研华	缓冲区错误漏洞（CNNVD-201906-719）
		CNNVD-201906-1078		
		CNNVD-201906-719		
		CNNVD-201906-724		
		CNNVD-201906-114	HPE	
		CNNVD-201906-618	Facebook	
		CNNVD-201906-619		
		CNNVD-201906-621		
		CNNVD-201906-622		
		CNNVD-201906-653	HP	
		CNNVD-201906-918	Cesanta	
9	访问控制错误	CNNVD-201906-1044	Cisco	Cisco Data Center Network Manager 访问控制错误漏洞（CNNVD-201906-1044）
		CNNVD-201906-175	HPE	
		CNNVD-201906-679	Citrix Systems	
		CNNVD-201906-733	Oracle	
		CNNVD-201906-765	Nagios	
10	代码问题	CNNVD-201906-033	WordPress	Adobe ColdFusion 代码问题漏洞（CNNVD-201906-520）
		CNNVD-201906-068	Google	
		CNNVD-201906-283	Optergy	
		CNNVD-201906-518	Adobe	
		CNNVD-201906-520		
		CNNVD-201906-577	Artifex Software	
		CNNVD-201906-587	BD	
		CNNVD-201906-802	Cisco	
11	安全特征问题	CNNVD-201906-431	Microsoft	Microsoft Windows 安全特征问题漏洞（CNNVD-201906-431）
12	SQL 注入	CNNVD-201906-172	ZOHO	ZOHO ManageEngine Netflow Analyzer SQL 注入漏洞（CNNVD-201906-172）
		CNNVD-201906-299	Cloudera	
		CNNVD-201906-905	LiveZilla	
		CNNVD-201906-930		

1. Magento 注入漏洞（CNNVD-201906-971）

Magento 是美国 Magento 公司的一套开源的 PHP 电子商务系统。该系统提供权限管理、搜索引擎和支付网关等功能。

Magento 2.1.18 之前的 2.1 版本、2.2.9 之前的 2.2 版本和 2.3.2 之

前的 2.3 版本中存在注入漏洞。攻击者可利用该漏洞导致 MySQL 出错。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13

2. WAGO Industrial Managed Switches 852-303、852-1305 和 852-1505 信任管理问题漏洞（CNNVD-201906-586）

WAGO Industrial Managed Switches 852-303 等都是德国 WAGO 公司的一款工业管理型交换机。

WAGO Industrial Managed Switches 852-303 1.2.2.S0 之前版本、852-1305 1.1.6.S0 之前版本和 852-1505 1.1.5.S0 之前版本中存在信任管理问题漏洞，该漏洞源于程序使用了硬编码账户和密码。攻击者可借助该账户利用该漏洞进行登录。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.wago.com/global/download/public/SA-SYS-2019-002.pdf/SA-SYS-2019-002.pdf

3. Intel RAID Web Console 3 输入验证错误漏洞（CNNVD-201906-575）

Intel RAID Web Console 3（RWC3）是美国英特尔（Intel）公司的一款基于 Web 的、为 Intel RAID 产品提供监控、维护、故障处理和配置功能的应用程序。

Intel RWC3 4.186 及之前版本中的 service API 存在输入验证错误

漏洞，该漏洞源于程序没有充分验证会话。攻击者可利用该漏洞提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00259.html

4. AU Optronics Solar Data Recorder 授权问题漏洞（CNNVD-201906-031）

AU Optronics Solar Data Recorder 是中国台湾 AU Optronics 公司的一款光伏数据记录器。

AU Optronics Solar Data Recorder 1.3.0 之前版本中存在授权问题漏洞，该漏洞源于 Web 门户使用了 HTTP 基本认证并将用户密码和用户名以明文形式显示在 WWW-Authenticate 属性中。攻击者可利用该漏洞获取密码和用户名，进而进行登录。

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.auo.com/

5. Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-201906-1029）

Cisco Data Center Network Manager 是美国思科（Cisco）公司的一套数据中心管理系统。该系统适用于 Cisco Nexus 和 MDS 系列交换机，提供存储可视化、配置和故障排除等功能。

Cisco Data Center Network Manager 11.2(1)之前版本中的基于 Web 的管理界面存在权限许可和访问控制问题漏洞，该漏洞源于不正确的

权限设置。攻击者可通过上传特制的数据利用该漏洞写入任意文件并 root 权限执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-codex

6. ZTE MF920 命令注入漏洞（CNNVD-201906-371）

ZTE MF920 是中国中兴通讯（ZTE）公司的一款无线调制解调器设备。

ZTE MF920 BD_R218V2.4 之前版本中存在命令注入漏洞。攻击者可利用该漏洞执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010686

7. HPE Intelligent Management Center PLAT 路径遍历漏洞（CNNVD-201906-133）

HPE Intelligent Management Center（iMC）PLAT 是美国惠普企业公司（Hewlett Packard Enterprise，HPE）的一套网络智能管理中心解决方案。该解决方案可提供整个网络范围的可视性，实现对资源、服务和用户的全面管理。

HPE iMC PLAT 7.3 E0506P09 之前版本中存在路径遍历漏洞。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://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us

8. Advantech WebAccess/SCADA 缓冲区错误漏洞（CNNVD-201906-719）

Advantech WebAccess/SCADA 是中国台湾研华（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 8.4.0 版本中存在缓冲区错误漏洞。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，详情请关注厂商主页：

https://www.advantech.com/

9. Cisco Data Center Network Manager 访问控制错误漏洞（CNNVD-201906-1044）

Cisco Data Center Network Manager 是美国思科（Cisco）公司的一套数据中心管理系统。该系统适用于 Cisco Nexus 和 MDS 系列交换机，提供存储可视化、配置和故障排除等功能。

Cisco Data Center Network Manager 11.1(1)之前版本中基于 Web 的管理界面存在访问控制错误漏洞，该漏洞源于程序没有正确管理会话。远程攻击者可通过发送特制的 HTTP 请求利用该漏洞绕过身份验证并以管理权限执行任意操作。

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-20190626-dcnm-bypass

10. Adobe ColdFusion 代码问题漏洞（CNNVD-201906-520）

Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。

Adobe ColdFusion 2018 Update 4 及之前版本、ColdFusion 2016 Update 11 及之前版本和 ColdFusion 11 Update 19 及之前版本中存在代码问漏洞。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://helpx.adobe.com/security/products/coldfusion/apsb19-27.html

11. Microsoft Windows 安全特征问题漏洞（CNNVD-201906-431）

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。

Microsoft Windows 中存在安全特征绕过漏洞。攻击者可借助特制的身份验证请求利用该漏洞绕过安全限制。以下产品及版本受到影响：

- Microsoft Windows 10
- Microsoft Windows 10 版本 1607
- Microsoft Windows 10 版本 1703
- Microsoft Windows 10 版本 1709
- Microsoft Windows 10 版本 1803
- Microsoft Windows 10 版本 1809
- Microsoft Windows 10 版本 1903

- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows RT 8.1
- Microsoft Windows Server 2008 SP2
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 版本 1803
- Microsoft Windows Server 版本 1903

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-2019-1019

12. ZOHO ManageEngine Netflow Analyzer SQL 注入漏洞（CNNVD-201906-172）

ZOHO ManageEngine Netflow Analyzer 是美国卓豪（ZOHO）公司的一套基于 Web 的带宽监控工具。该产品主要用于带宽监控和流量分析。

ZOHO ManageEngine NetFlow Analyzer 12.3 版本中的 /client/api/json/v2/nfareports/compareReport 存在 SQL 注入漏洞。远程攻击者可借助‘DeviceID’参数利用该漏洞执行任意的 SQL 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.manageengine.com/products/netflow/readme.html#124029

1.4.2 高危漏洞实例

本月高危漏洞共 497 个，其中重点漏洞实例如表 6 所示。

表 6　2019 年 6 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	命令注入	CNNVD-201906-014	NETGEAR	NETGEAR Insight 命令注入漏洞（CNNVD-201906-014）
2	资源管理错误	CNNVD-201906-066	Google	Adobe Flash Player 资源管理错误漏洞（CNNVD-201906-509）
		CNNVD-201906-076		
		CNNVD-201906-240		
		CNNVD-201906-242		
		CNNVD-201906-625		
		CNNVD-201906-278	VMware	
		CNNVD-201906-509	Adobe	
		CNNVD-201906-605	Qualcomm	
		CNNVD-201906-609		
		CNNVD-201906-680	Linux	
		CNNVD-201906-682		
		CNNVD-201906-683		
		CNNVD-201906-834	Phoenix Contact	
		CNNVD-201906-852	Apache	
3	注入	CNNVD-201906-107	Copperfasten 4Technologies	IBM Maximo Asset Management 注入漏洞（CNNVD-201906-689）

		CNNVD-201906-111	HPE	
		CNNVD-201906-112		
		CNNVD-201906-115		
		CNNVD-201906-116		
		CNNVD-201906-117		
		CNNVD-201906-118		
		CNNVD-201906-120		
		CNNVD-201906-122		
		CNNVD-201906-125		
		CNNVD-201906-130		
		CNNVD-201906-136		
		CNNVD-201906-138		
		CNNVD-201906-147		
		CNNVD-201906-152		
		CNNVD-201906-192		
		CNNVD-201906-195		
		CNNVD-201906-196		
		CNNVD-201906-197		
		CNNVD-201906-198		
		CNNVD-201906-199		
		CNNVD-201906-205		
		CNNVD-201906-229		
		CNNVD-201906-689	IBM	
		CNNVD-201906-929	LiveZilla	
4	信息泄露	CNNVD-201906-044	IBM	Cisco WebEx Meetings Server 信息泄露漏洞（CNNVD-201906-160）
		CNNVD-201906-856		
		CNNVD-201906-053		
		CNNVD-201906-160	Cisco	

		CNNVD-201906-376	中兴通讯	
		CNNVD-201906-525	SAP	
		CNNVD-201906-902	Micro Focus	
		CNNVD-201906-954	Magento	
5	信任管理问题	CNNVD-201906-208	HPE	IBM Cloud Private 信任管理问题漏洞（CNNVD-201906-533）
		CNNVD-201906-288	Optergy	
		CNNVD-201906-298	Samsung	
		CNNVD-201906-387	CloudBees	
		CNNVD-201906-533	IBM	
		CNNVD-201906-585		
		CNNVD-201906-849	Pivotal Software	
6	输入验证错误	CNNVD-201906-166	SweetScape Software	NVIDIA Vibrante Linux 输入验证错误漏洞（CNNVD-201906-225）
		CNNVD-201906-168		
		CNNVD-201906-615	Qualcomm	
		CNNVD-201906-617		
		CNNVD-201906-225	NVIDIA	
		CNNVD-201906-882	Netflix	
		CNNVD-201906-443	Microsoft	
		CNNVD-201906-447		
		CNNVD-201906-478		
		CNNVD-201906-681	Linux	
		CNNVD-201906-045	IBM	
		CNNVD-201906-245		
		CNNVD-201906-123	HPE	
		CNNVD-201906-124		
		CNNVD-201906-126		
		CNNVD-201906-137		

		CNNVD-201906-139		
		CNNVD-201906-140		
		CNNVD-201906-146		
		CNNVD-201906-148		
		CNNVD-201906-149		
		CNNVD-201906-150		
		CNNVD-201906-151		
		CNNVD-201906-180		
		CNNVD-201906-191		
		CNNVD-201906-193		
		CNNVD-201906-200		
		CNNVD-201906-203		
		CNNVD-201906-210		
		CNNVD-201906-212		
		CNNVD-201906-214		
		CNNVD-201906-218		
		CNNVD-201906-226		
		CNNVD-201906-227		
		CNNVD-201906-228		
		CNNVD-201906-559	Fuji Electric	
		CNNVD-201906-686	Dell	
		CNNVD-201906-158	Cisco	
		CNNVD-201906-159		
		CNNVD-201906-799		
7	授权问题	CNNVD-201906-069	Google	Intel Omni-Path Fabric Manager GUI 授权问题漏洞（CNNVD-201906-576）
		CNNVD-201906-215	HPE	
		CNNVD-201906-219		
		CNNVD-201906-531	Siemens	

		CNNVD-201906-576	Intel	
		CNNVD-201906-580	Johnson Controls	
		CNNVD-201906-717	ZOHO	
		CNNVD-201906-855	Sony	
8	权限许可和访问控制问题	CNNVD-201906-524	Siemens	Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-201906-1021）
		CNNVD-201906-528		
		CNNVD-201906-254	Rancher Labs	
		CNNVD-201906-041	Quest Software	
		CNNVD-201906-406	Microsoft	
		CNNVD-201906-407		
		CNNVD-201906-408		
		CNNVD-201906-409		
		CNNVD-201906-410		
		CNNVD-201906-411		
		CNNVD-201906-414		
		CNNVD-201906-415		
		CNNVD-201906-416		
		CNNVD-201906-418		
		CNNVD-201906-420		
		CNNVD-201906-422		
		CNNVD-201906-427		
		CNNVD-201906-432		
		CNNVD-201906-433		
		CNNVD-201906-459		
		CNNVD-201906-479		
		CNNVD-201906-481		
		CNNVD-201906-484		

		CNNVD-201906-487		
		CNNVD-201906-488		
		CNNVD-201906-489		
		CNNVD-201906-491		
		CNNVD-201906-526	Intel	
		CNNVD-201906-564		
		CNNVD-201906-636	IBM	
		CNNVD-201906-857		
		CNNVD-201906-194	HPE	
		CNNVD-201906-924	HP	
		CNNVD-201906-071	Google	
		CNNVD-201906-072		
		CNNVD-201906-074		
		CNNVD-201906-078		
		CNNVD-201906-1021	Cisco	
		CNNVD-201906-798		
		CNNVD-201906-795		
		CNNVD-201906-850	Dell	
9	配置错误	CNNVD-201906-070	Qualcomm	多款 Qualcomm 产品配置错误漏洞（CNNVD-201906-070）
10	命令注入	CNNVD-201906-025	Micro Focus	Adobe Campaign Classic 命令注入漏洞（CNNVD-201906-505）
		CNNVD-201906-087	Geutebrück	
		CNNVD-201906-088		
		CNNVD-201906-1064	McAfee	
		CNNVD-201906-1066		
		CNNVD-201906-119	HPE	
		CNNVD-201906-121		

		CNNVD-201906-127		
		CNNVD-201906-128		
		CNNVD-201906-131		
		CNNVD-201906-132		
		CNNVD-201906-142		
		CNNVD-201906-143		
		CNNVD-201906-145		
		CNNVD-201906-176		
		CNNVD-201906-202		
		CNNVD-201906-204		
		CNNVD-201906-224		
		CNNVD-201906-256	Rancher Labs	
		CNNVD-201906-373	中兴通讯	
		CNNVD-201906-505	Adobe	
		CNNVD-201906-630	OrangeHRM	
		CNNVD-201906-771	Sony	
		CNNVD-201906-797	Cisco	
		CNNVD-201906-936	联想	
11	路径遍历	CNNVD-201906-1068	McAfee	Advantech WebAccess/SCADA 路径遍历漏洞（CNNVD-201906-1074）
		CNNVD-201906-1074	研华	
		CNNVD-201906-1153	群晖科技	
		CNNVD-201906-774	Sony	
		CNNVD-201906-892	ABB	
		CNNVD-201906-966	IBM	
12	跨站脚本	CNNVD-201906-529	Intel	Intel Rapid Storage Technology Enterprise Intel Accelerated Storage Manager 跨站脚本漏洞
		CNNVD-201906-179	HPE	

				（CNNVD-201906-529）
13	跨站请求伪造	CNNVD-201906-372	中兴通讯	IBM Cloud Private 跨站请求伪造漏洞（CNNVD-201906-634）
		CNNVD-201906-942	联想	
		CNNVD-201906-634	IBM	
		CNNVD-201906-779		
		CNNVD-201906-652	HP	
		CNNVD-201906-390	CloudBees	
		CNNVD-201906-156	Cisco	
		CNNVD-201906-546		
		CNNVD-201906-790		
		CNNVD-201906-792		
		CNNVD-201906-869	Bobronix	
14	缓冲区错误	CNNVD-201906-1076	研华	Phoenix Contact Automation Worx Software Suite PC Worx、PC Worx Express 和 Config+ 缓冲区错误漏洞（CNNVD-201906-829）
		CNNVD-201906-556	大华	
		CNNVD-201906-273	VMware	
		CNNVD-201906-333	SolarWinds	
		CNNVD-201906-338		
		CNNVD-201906-339		
		CNNVD-201906-606	Qualcomm	
		CNNVD-201906-608		
		CNNVD-201906-616		
		CNNVD-201906-620		
		CNNVD-201906-829	Phoenix Contact	
		CNNVD-201906-840		
		CNNVD-201906-281	Panasonic	
		CNNVD-201906-601	Mozilla	
		CNNVD-201906-602		
		CNNVD-201906-604		

		CNNVD-201906-412	Microsoft	
		CNNVD-201906-413		
		CNNVD-201906-421		
		CNNVD-201906-425		
		CNNVD-201906-428		
		CNNVD-201906-448		
		CNNVD-201906-450		
		CNNVD-201906-452		
		CNNVD-201906-453		
		CNNVD-201906-454		
		CNNVD-201906-456		
		CNNVD-201906-457		
		CNNVD-201906-465		
		CNNVD-201906-466		
		CNNVD-201906-467		
		CNNVD-201906-468		
		CNNVD-201906-469		
		CNNVD-201906-471		
		CNNVD-201906-472		
		CNNVD-201906-473		
		CNNVD-201906-474		
		CNNVD-201906-475		
		CNNVD-201906-476		
		CNNVD-201906-477		
		CNNVD-201906-482		
		CNNVD-201906-498		
		CNNVD-201906-516		
		CNNVD-201906-903	Linux	

		CNNVD-201906-1031	ImageMagick Studio	
		CNNVD-201906-1032		
		CNNVD-201906-1033		
		CNNVD-201906-1092	IBM	
		CNNVD-201906-1120		
		CNNVD-201906-178	HPE	
		CNNVD-201906-201		
		CNNVD-201906-651	HP	
		CNNVD-201906-067	Google	
		CNNVD-201906-080		
		CNNVD-201906-081		
		CNNVD-201906-610	Embedthis Software	
		CNNVD-201906-806	Cisco	
		CNNVD-201906-904	ABB	
15	后置链接	CNNVD-201906-034	Facebook	Facebook osquery 后置链接漏洞（CNNVD-201906-034）
16	访问控制错误	CNNVD-201906-054	IBM	Odoo 访问控制错误漏洞（CNNVD-201906-1104）
		CNNVD-201906-073	Qualcomm	
		CNNVD-201906-1104	Odoo	
		CNNVD-201906-1105		
		CNNVD-201906-519	Siemens	
		CNNVD-201906-521		
		CNNVD-201906-530	Intel	
		CNNVD-201906-810	Red Hat	
		CNNVD-201906-812		
		CNNVD-201906-816	蓝智科技	

17	代码问题	CNNVD-201906-252	Sitecore	Sitecore Experience Platform 代码问题漏洞（CNNVD-201906-252）
		CNNVD-201906-103	Prima Systems	
		CNNVD-201906-931	PC-Doctor Toolbox	
		CNNVD-201906-279	Panasonic	
		CNNVD-201906-492	Microsoft	
		CNNVD-201906-039	Linux	
		CNNVD-201906-040		
		CNNVD-201906-051		
		CNNVD-201906-599		
		CNNVD-201906-047	IBM	
		CNNVD-201906-134	HPE	
		CNNVD-201906-141		
		CNNVD-201906-624	Electronic Arts	
		CNNVD-201906-271	Dell	
		CNNVD-201906-391	CloudBees	
18	操作系统命令注入	CNNVD-201906-1158	群晖科技	Synology Calendar 操作系统命令注入漏洞（CNNVD-201906-1158）
		CNNVD-201906-809	Cisco	
		CNNVD-201906-837	Sophos	
		CNNVD-201906-838		
19	参数注入	CNNVD-201906-611	Atlassian	Atlassian Sourcetree 参数注入漏洞（CNNVD-201906-611）
20	安全特征问题	CNNVD-201906-174	HPE	Microsoft Windows Secure Kernel Mode 安全特征问题漏洞（CNNVD-201906-451）
		CNNVD-201906-451	Microsoft	
21	SQL 注入	CNNVD-201906-1150	群晖科技	Magento SQL 注入漏洞（CNNVD-201906-983）
		CNNVD-201906-177	HPE	
		CNNVD-201906-181		

		CNNVD-201906-182		
		CNNVD-201906-183		
		CNNVD-201906-184		
		CNNVD-201906-185		
		CNNVD-201906-186		
		CNNVD-201906-187		
		CNNVD-201906-188		
		CNNVD-201906-189		
		CNNVD-201906-190		
		CNNVD-201906-836	Sophos	
		CNNVD-201906-983	Magento	
		CNNVD-201906-984		

1. NETGEAR Insight 命令注入漏洞（CNNVD-201906-014）

NETGEAR Insight 是美国网件（NETGEAR）公司的一套基于云的管理平台。该平台支持设置和配置 NETGEAR Insight 托管接入点、交换机和 ReadyNAS 设备等。

NETGEAR Insight 5.6 之前版本中存在命令注入漏洞。攻击者可利用该漏洞注入命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://kb.netgear.com/000060977/Security-Advisory-for-Post-Authentication-Command-Injection-on-Insight-Cloud-PSV-2018-0366

2. Adobe Flash Player 资源管理错误漏洞（CNNVD-201906-509）

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应

用程序、内容和视频。

Adobe Flash Player 中存在资源管理错误漏洞。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。以下产品及版本受到影响：

- 基于 Windows、macOS 和 Linux 平台的 Adobe Flash Player Desktop Runtime 32.0.0.192 及之前版本
- 基于 Windows、macOS 、Linux 和 Chrome OS 平台的 Adobe Flash Player for Google Chrome 32.0.0.192 及之前版本
- 基于 Windows 10 和 8.1 平台的 Adobe Flash Player for Microsoft Edge 和 Internet Explorer 11 32.0.0.192 及之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/flash-player/apsb19-30.html

3. IBM Maximo Asset Management 注入漏洞（CNNVD-201906-689）

IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。

IBM Maximo Asset Management 7.6 版本中存在注入漏洞。远程攻击者可利用该漏洞在系统上执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www-01.ibm.com/support/docview.wss?uid=ibm10887557

4. Cisco WebEx Meetings Server 信息泄露漏洞（CNNVD-201906-160）

Cisco WebEx Meetings Server（CWMS）是 WebEx 会议方案中的一套包含音频、视频和 Web 会议的多功能会议解决方案。

Cisco CWMS 中的基于 Web 的管理界面存在信息泄露漏洞，该漏洞源于程序没有进行正确的访问控制。攻击者可通过发送恶意的请求利用该漏洞访问敏感的系统信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvn76141

5. IBM Cloud Private 信任管理问题漏洞（CNNVD-201906-533）

IBM Cloud Private 是美国 IBM 公司的一套企业私有云解决方案。

IBM Cloud Private 1.0.0 版本至 3.0.1 版本中存在信任管理问题漏洞，该漏洞源于程序将用户凭证存储为明文形式。本地攻击者可利用该漏洞读取敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www-01.ibm.com/support/docview.wss?uid=ibm10886591

6. NVIDIA Vibrante Linux 输入验证错误漏洞（CNNVD-201906-225）

NVIDIA Vibrante Linux 是美国英伟达（NVIDIA）公司的一套用于 Drive PX2（开放式人工智能车辆计算平台）的 Linux 发行版。

NVIDIA Vibrante Linux 1.1 版本、2.0 版本和 2.2 版本中存在输入验证错误漏洞。攻击者可利用该漏洞造成拒绝服务或泄露信息。

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.nvidia.com/

7. Intel Omni-Path Fabric Manager GUI 授权问题漏洞（CNNVD-201906-576）

Intel Omni-Path Fabric Manager GUI 是美国英特尔（Intel）公司的一款用于 Intel Omni-Path Fabric（通信架构）管理的图形界面。

Intel Omni-Path Fabric Manager GUI 10.9.2.1.1 之前版本中的安装程序存在授权问题漏洞。本地攻击者可利用该漏洞提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00257.html

8. Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-201906-1021）

Cisco Data Center Network Manager 是美国思科（Cisco）公司的一套数据中心管理系统。该系统适用于 Cisco Nexus 和 MDS 系列交换机，提供存储可视化、配置和故障排除等功能。

Cisco Data Center Network Manager 11.2(1)之前版本中基于 Web 的管理界面存在权限许可和访问控制问题漏洞，该漏洞源于不正确的权限设置。远程攻击者可通过将该界面连接到受影响设备并请求 URLs 利用该漏洞获取敏感信息的访问权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-file-dwnld

9. 多款 Qualcomm 产品配置错误漏洞（CNNVD-201906-070）

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司的一款中央。处理器（CPU）产品。

多款 Qualcomm 产品中的 Kernel 存在配置错误漏洞。攻击者可利用该漏洞泄露信息。以下产品及版本受到影响：

- Qualcomm IPQ8074

- Qualcomm MDM9150
- Qualcomm MDM9206
- Qualcomm MDM9607
- Qualcomm MDM9650
- Qualcomm MSM8996AU
- Qualcomm QCA8081
- Qualcomm QCS605
- Qualcomm 215
- Qualcomm SD 210
- Qualcomm SD 212
- Qualcomm SD 205
- Qualcomm SD 425
- Qualcomm SD 427
- Qualcomm SD 430
- Qualcomm SD 435
- Qualcomm SD 439
- Qualcomm SD 429
- Qualcomm SD 450
- Qualcomm SD 625
- Qualcomm SD 632
- Qualcomm SD 636
- Qualcomm SD 650/52

- Qualcomm SD 675
- Qualcomm SD 712
- Qualcomm SD 710
- Qualcomm SD 670
- Qualcomm SD 730
- Qualcomm SD 820
- Qualcomm SD 820A
- Qualcomm SD 835
- Qualcomm SD 845
- Qualcomm SD 850
- Qualcomm SD 855
- Qualcomm SD 8CX
- Qualcomm SDA660
- Qualcomm SDM439
- Qualcomm SDM630
- Qualcomm SDM660
- Qualcomm Snapdragon_High_Med_2016
- Qualcomm SXR1130

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

10. Adobe Campaign Classic 命令注入漏洞（CNNVD-201906-505）

Adobe Campaign Classic（ACC）是美国奥多比（Adobe）公司的一套跨渠道客户体验营销平台。该平台具有实时交互管理、Adobe

Experience Cloud 集成、数据管理和集成等功能。

基于 Windows 和 Linux 平台的 Adobe Campaign Classic 18.10.5-8984 及之前版本中存在命令注入漏洞。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://helpx.adobe.com/security/products/campaign/apsb19-28.html

11. Advantech WebAccess/SCADA 路径遍历漏洞

（CNNVD-201906-1074）

Advantech WebAccess/SCADA 是中国台湾研华（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 8.3.5 及之前版本中存在路径遍历漏洞，该漏洞源于程序没有正确验证用户提供的文件路径。攻击者可利用该漏洞删除文件。

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.advantech.com/

12. Intel Rapid Storage Technology Enterprise Intel Accelerated Storage Manager 跨站脚本漏洞

（CNNVD-201906-529）

Intel Rapid Storage Technology enterprise（RSTe）是美国英特尔（Intel）公司的一款快速存储技术。Intel Accelerated Storage Manager 是其中的一个加速存储管理器。

Intel RSTe 中的 Intel Accelerated Storage Manager 存在跨站脚本漏

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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00226.html

13. IBM Cloud Private 跨站请求伪造漏洞（CNNVD-201906-634）

IBM Cloud Private 是美国 IBM 公司的一套企业私有云解决方案。该产品主要基于 Kubernetes 和容器技术搭建。

IBM Cloud Private 中存在跨站请求伪造漏洞。攻击者可利用该漏洞执行恶意的未授权操作。以下产品及版本受到影响：

- IBM Cloud Private 2.1.x 版本
- IBM Cloud Private 3.1.0 版本
- IBM Cloud Private 3.1.1 版本
- IBM Cloud Private 3.1.2 版本

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://www.ibm.com/support/docview.wss?uid=ibm10885434

14. Phoenix Contact Automation Worx Software Suite PC Worx、PC Worx Express 和 Config+ 缓冲区错误漏洞(CNNVD-201906-829)

Phoenix Contact Automation Worx Software Suite 是德国菲尼克斯电气（Phoenix Contact）公司的一套自动化 Worx 软件套件。PC Worx 是其中的一套控制器编程软件。Config+是其中的一套用于配置和诊断 INTERBUS 系统的软件。

Phoenix Contact Automation Worx Software Suite 中的 PC Worx 1.86 及之前版本、PC Worx Express 1.86 及之前版本和 Config+ 1.86 及之前

版本存在缓冲区错误漏洞。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.phoenixcontact.com/

15. Facebook osquery 后置链接漏洞（CNNVD-201906-034）

Facebook osquery 是美国 Facebook 公司的一款基于 SQL 的、开源的操作系统检测和监控框架。

Facebook osquery 3.4.0 之前版本中存在后置链接漏洞。攻击者可利用该漏洞以 SYSTEM 权限加载恶意的二进制文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.facebook.com/security/advisories/cve-2019-3567

16. Odoo 访问控制错误漏洞（CNNVD-201906-1104）

Odoo 是比利时 Odoo 公司的一套开源商业系统。

Odoo 9.0 版本（社区版和企业版）中的密码加密模块存在访问控制错误漏洞。攻击者可利用该漏洞修改其他用户的密码。

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/odoo/odoo/issues/32507

17. Sitecore Experience Platform 代码问题漏洞（CNNVD-201906-252）

Sitecore Experience Platform（XP）是丹麦 Sitecore 公司的一套客户数字体验平台。

Sitecore Experience Platform (XP) 9.1.1 之前版本中存在代码问题漏洞。攻击者可借助特制的序列化对象利用该漏洞执行操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://dev.sitecore.net/Downloads/Sitecore%20Experience%20Platfo

rm/91/Sitecore%20Experience%20Platform%2091%20Update1/Release%20Notes

18. Synology Calendar 操作系统命令注入漏洞（CNNVD-201906-1158）

Synology Calendar 是中国台湾群晖科技（Synology）公司的一款运行在 Synology NAS（网络存储服务器）设备上的文件保护程序。

Synology Calendar 2.3.1-0617 之前版本中的 drivers_syno_import_user.php 文件存在操作系统命令注入漏洞。远程攻击者可利用该漏洞执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.synology.com/security/advisory/Synology_SA_19_12

19. Atlassian Sourcetree 参数注入漏洞（CNNVD-201906-611）

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。

Atlassian Sourcetree 3.1.3 之前版本（用于 Windows URI 处理器）中存在参数注入漏洞。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，补丁获取链接：https://jira.atlassian.com/browse/SRCTREEWIN-11917

20. Microsoft Windows Secure Kernel Mode 安全特征问题漏洞（CNNVD-201906-451）

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。

Microsoft Windows Secure Kernel Mode 中存在安全特征问题漏洞，该漏洞源于程序没有正确处理内存对象。攻击者可通过运行特制的应用程序利用该漏洞绕过安全限制，执行未授权的操作。以下产品及版本受到影响：

- Microsoft Windows 10 版本 1809
- Microsoft Windows Server 2019

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-2019-1044

21. Magento SQL 注入漏洞（CNNVD-201906-983）

Magento 是美国 Magento 公司的一套开源的 PHP 电子商务系统。该系统提供权限管理、搜索引擎和支付网关等功能。

Magento Open Source 1.9.4.2 之前版本和 Magento Commerce 1.14.4.2 之前版本中的企业登录功能存在 SQL 注入漏洞。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://magento.com/security/patches/supee-11155

二、接报漏洞情况

本月接报漏洞共计 3662 个，其中信息技术产品漏洞（通用型漏洞）57 个，网络信息系统漏洞（事件型漏洞）3605 个。

表 7 2019 年 6 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	2026	0	2026
2	网神信息技术（北京）股份有限公司	1296	0	1296
3	内蒙古奥创科技有限公司	164	12	152
4	中新网络信息安全股份有限公司	80	0	80
5	北京数字观星科技有限公司	51	0	51
6	山东新潮信息技术有限公司	42	0	42
7	广州锦行网络科技有限公司	21	1	20
8	北京圣溥润高新技术服份有限公司	19	0	19
9	新华三技术有限公司	15	0	15
10	国发中新（北京）科技发展有限公司	15	0	15
11	西安交大捷普网络科技有限公司	14	0	14
12	福建经联网络技术有限公司	11	0	11
13	西安四叶草信息技术有限公司	11	0	11
14	新华三技术有限公司	10	10	0
15	北京神州绿盟科技有限公司安全研究部	6	6	0
16	北京启明星辰信息安全技术有限公司	5	5	0
17	杭州木链物联网科技有限公司	5	5	0
18	杭州安恒信息技术股份有限公司	3	3	0
19	北京安信天行科技有限公司	2	0	2
20	东方电气启明星辰工控信息安全联合实验室	2	2	0
21	广州万方计算机科技有限公司	2	2	0

22	武汉绿色网络信息服务有限责任公司	2	2	0
23	福建经联网络技术有限公司	2	2	0
24	北京威努特技术有限公司	1	1	0
25	西安电子科技大学	1	1	0
26	长扬科技（北京）有限公司	1	0	1
27	北京天融信网络安全技术有限公司	1	1	0
28	工业和信息化部电子第五研究所信息安全研究中心	1	1	0
29	北京邮电大学	1	1	0
30	北京山石网科信息技术有限公司	1	1	0
报送总计		3662	57	3605

三、重大漏洞预警

3.1 Linux 和 FreeBSD 内核多个安全漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Linux 和 FreeBSD 内核多个安全漏洞（CNNVD-201906-681、CVE-2019-11477）（CNNVD-201906-682、CVE-2019-11478）（CNNVD-201906-683、CVE-2019-11479）（CNNVD-201906-703、CVE-2019-5599）情况的报送。攻击者可以远程利用这些漏洞，造成 Linux 和 FreeBSD 内核崩溃，从而导致拒绝服务。Linux 多个版本受漏洞影响。目前，Ubuntu 和 RedHat 已发布漏洞修复补丁，暂未发布补丁的版本可通过临时修补措施缓解漏洞带来的危害，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

2019 年 6 月 18 日，Netflix 安全团队发布《Linux 和 FreeBSD 内核：多个基于 TCP 的远程拒绝服务漏洞公告》。报告中公布了相关漏洞（CNNVD-201906-681、CVE-2019-11477）（CNNVD-201906-682、CVE-2019-11478 ）（ CNNVD-201906-683 、 CVE-2019-11479 ）（CNNVD-201906-703、CVE-2019-5599）的细节。攻击者可通过发送精心设计的 SACK 序列来利用上述漏洞，造成 Linux 和 FreeBSD 内核崩溃，从而导致拒绝服务。

漏洞危害

成功利用该漏洞的攻击者可以造成 Linux 和 FreeBSD 内核崩溃，从而导致拒绝服务。Linux 多个版本受漏洞影响，具体影响版本如下：

CNNVD-201906-681、CVE-2019-11477 影响 Linux 2.6.29 以上的内核版本
CNNVD-201906-682、CVE-2019-11478 影响所有 Linux 版本
CNNVD-201906-683、CVE-2019-11479 影响所有 Linux 版本
CNNVD-201906-703、CVE-2019-5599 影响使用 RACK TCP 堆栈的 FreeBSD 12 版本

修复措施

目前，Ubuntu 和 RedHat 已发布漏洞修复补丁，暂未发布补丁的版本可通过临时修补措施缓解漏洞带来的危害，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。具体措施如下：

（1）CNNVD-201906-681、CVE-2019-11477 漏洞修复补丁

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001/PATCH_net_1_4.patch

Linux 内核版本>=4.14 需要打第二个补丁

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001/PATCH_net_1a.patch

（2）Ubuntu 和 RedHat 系统的修复方案

Ubuntu 用户可以使用如下命令更新（更新完成后需要重启生效）：

```
$ sudo apt-get update
$ sudo apt-get dist-upgrade
```

RedHat 用户可以使用如下命令更新（更新完成后需要重启生效）：

```
yum install -y yum-security
yum --security check-update
yum update --security
```

（3）其它漏洞临时修补措施

对于暂时无法更新内核或者重启的用户，可以使用如下缓解措施。

临时禁用易受攻击的组件：

```
# echo 0 > /proc/sys/net/ipv4/tcp_sack

或者

# sysctl -w net.ipv4.tcp_sack=0
```

或者使用 iptables 删除可能利用此漏洞的流量：

```
# iptables -I INPUT -p tcp --tcp-flags SYN SYN -m tcpmss --mss
1:500 -j DROP

# ip6tables -I INPUT -p tcp --tcp-flags SYN SYN -m tcpmss --mss
1:500 -j DROP

# iptables -nL -v

# ip6tables -nL -v
```

3.2 致远 OA 远程代码执行漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于致远 OA 远程代码执行漏洞（CNNVD-201906-1049）的报送。成功利用该漏洞的攻击者可以远程执行恶意代码。已确认 A8 V7.0 SP3、A8 V6.1 SP2 版本受漏洞影响，其余版本也可能存在受影响的风险。目前，官方表示修复补丁将在近期发布，暂时可以通过临时修补措施缓解漏洞带来的危害，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

致远是用友下属的子公司，从事 OA 办公自动化软件的开发销售与服务工作，致远 OA 是一款协同管理软件，在各中、大型企业机构中广泛使用。

致远 OA 存在远程代码执行漏洞（CNNVD-201906-1049），攻击者通过精心构造 POST 数据来上传恶意文件，提升服务器权限，从而控制服务器或对系统造成破坏。

漏洞危害

成功利用漏洞的攻击者可以在未授权的情况下实现恶意文件上传，提升服务器权限，从而控制服务器或对系统造成破坏。

安全建议

目前，厂商表示修复补丁将在近期发布，暂时可以通过临时修补措施缓解漏洞带来的危害，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。应对措施如下：

（1）及时与厂商联系，按照厂商指导获取漏洞修复补丁（官方补丁获取地址 http://support.seeyon.com）；

（2）采取临时修补措施缓解漏洞带来的危害，通过 ACL 禁止外网对“/seeyon/htmlofficeservlet”路径的访问。