北京师范大学网络信息安全通告

2019 年 7 月报告

北京师范大学信息网络中心

2019 年 8 月

目录

漏洞态势 1
1. 公开漏洞情况 1
1.1. 漏洞增长概况 1
1.2. 漏洞分布情况 2
1.2.1. 漏洞厂商分布 2
1.2.2. 漏洞产品分布 2
1.2.3. 漏洞类型分布 3
1.2.4. 漏洞危害等级分布 4
1.3. 漏洞修复情况 5
1.3.1. 整体修复情况 5
1.3.2. 厂商修复情况 6
1.4. 重要漏洞实例 6
1.4.1. 超危漏洞实例 6
1.4.2. 高危漏洞实例 17
2. 接报漏洞情况 41
3. 重大漏洞预警 44
3.1. Linux 和FreeBSD 内核多个安全漏洞预警 44
3.2. 致远OA 远程代码执行漏洞预警 45

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2019 年 7 月份新增安全漏洞共 1670 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 158 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 14.19%。本月新增漏洞中，超危漏洞 209 个、高危漏洞 589 个、中危漏洞 762 个、低危漏洞 110 个，相应修复率分别为 66.51%、80.31%、77.56%以及 78.18%。合计 1289 个漏洞已有修复补丁发布，本月整体修复率 77.19%。

截至 2019 年 7 月 31 日，CNNVD 采集漏洞总量已达 129539 个。

1.1 漏洞增长概况

2019 年 7 月新增安全漏洞 1670 个，与上月（1307 个）相比增加了 27.78%。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 1344 个。

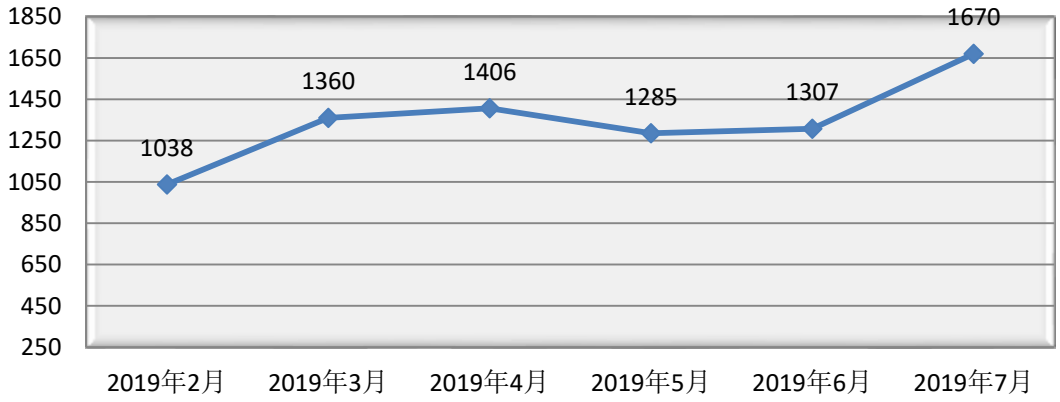

图 1 2019 年 2 月至 2019 年 7 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

7月厂商漏洞数量分布情况如表1所示，Oracle公司达到158个，占本月漏洞总量的9.46%。本月Oracle、苹果、Qualcomm等公司的漏洞数量均有所上升，HPE、微软等厂商的漏洞数量出现较不同程度的下降。

表1　2019年7月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量	所占比例
1	Oracle	158	9.46%
2	微软	77	4.61%
3	苹果	48	2.87%
4	Qualcomm	41	2.46%
5	cPanel	38	2.28%
6	IBM	34	2.04%
7	友讯	33	1.98%
8	GitLab	31	1.86%
9	谷歌	29	1.74%
10	思科	28	1.68%

1.2.2 漏洞产品分布

7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48条，其中桌面操作系统44条，服务器操作系统48条。本月Windows Server 1803漏洞数量最多，共41个，占主流操作系统漏洞总量的11.61%，排名第一。

表2　2019年7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 Server 1803	41

2	Windows Server 1903	40
3	Apple macOS	40
4	Windows 10	38
5	Apple iOS	35
6	Windows Server 2016	27
7	Windows Server 2012	22
8	Windows 7	21
9	Windows Server 2008	21
10	Windows 8.1	19
11	Linux Kernel	19
12	Windows Rt 8.1	18
13	Android	12

*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

7 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 14.19%。

表 32019 年 7 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区错误	237	14.19%
2	访问控制错误	193	11.56%
3	跨站脚本	185	11.08%
4	输入验证错误	160	9.58%
5	信息泄露	107	6.41%
6	代码问题	75	4.49%

7	资源管理错误	68	4.07%
8	权限许可和访问控制问题	65	3.89%
9	SQL 注入	56	3.35%
10	授权问题	52	3.11%
11	命令注入	49	2.93%
12	跨站请求伪造	47	2.81%
13	信任管理问题	44	2.63%
14	路径遍历	24	1.44%
15	加密问题	14	0.84%
16	数字错误	13	0.78%
17	处理逻辑错误	12	0.72%
18	安全特征问题	10	0.60%
19	注入	9	0.54%
20	竞争条件问题	9	0.54%
21	代码注入	8	0.48%
22	后置链接	8	0.48%
23	操作系统命令注入	8	0.48%
24	参数注入	6	0.36%
25	数据伪造问题	6	0.36%
26	格式化字符串错误	5	0.30%
27	日志信息泄露	3	0.18%
28	配置错误	2	0.12%
29	默认配置问题	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。7 月漏洞

危害等级分布如图 2 所示，其中超危漏洞 209 条，占本月漏洞总数的 12.51%。

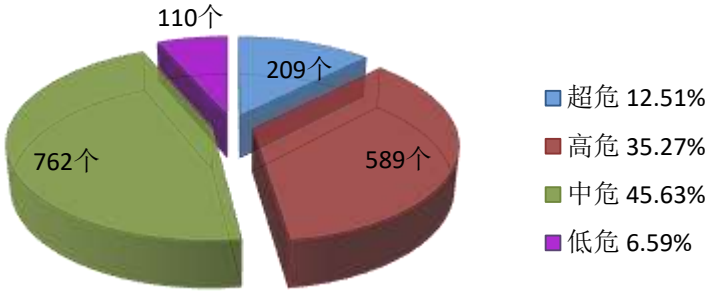

图 2　2019 年 7 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

7 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 80.31%，超高危漏洞修复率最低，比例为 66.51%。与上月相比，本月中、低危漏洞修复率有所上升，超危、高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 71.92% 上升至本月的 77.19%。

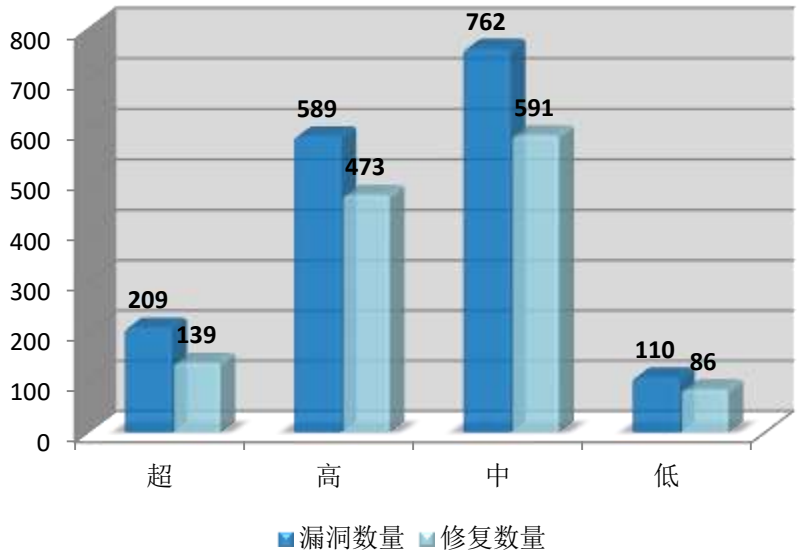

图 3　2019 年 7 月漏洞修复数量统计

1.3.2　厂商修复情况

7 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、微软、IBM 等十个厂商共 517 条漏洞，占本月漏洞总数的 30.96%，漏洞修复率为 95.74%，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、微软、苹果、Qualcomm 等公司本月漏洞修复率均为 100%，共 648 条漏洞已全部修复。

表 4　2019 年 7 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	158	158	100.00%
2	微软	77	77	100.00%
3	苹果	48	48	100.00%
4	Qualcomm	41	41	100.00%
5	cPanel	38	38	100.00%
6	IBM	34	33	97.06%
7	友讯	33	15	45.45%
8	GitLab	31	31	100.00%
9	谷歌	29	29	100.00%
10	思科	28	25	89.29%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 209 个，其中重要漏洞实例如表 5 所示。

表 5　2019 年 7 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	资源管理错误	CNNVD-201907-043	谷歌	Android System 组件资源管理错误漏洞（CNNVD-201907-043）
		CNNVD-201907-158	摩莎	
2	注入	CNNVD-201907-190	JetBrains	JetBrains YouTrack 插件注入漏洞（CNNVD-201907-190）
3	信息泄露	CNNVD-201907-078	Qualcomm	Moxa OnCell G3100-HSPA 信息泄露漏洞（CNNVD-201907-159）
		CNNVD-201907-159	摩莎	
		CNNVD-201907-508	HPE	
4	信任管理问题	CNNVD-201907-016	Prima Systems	Amcrest IPM-721S 信任管理问题漏洞（CNNVD-201907-200）
		CNNVD-201907-192	JetBrains	
		CNNVD-201907-193		
		CNNVD-201907-195	Amcrest	
		CNNVD-201907-200		
		CNNVD-201907-324	WolfVision	
		CNNVD-201907-375	Sonatype	
		CNNVD-201907-506	Arlo Technologies	
		CNNVD-201907-649	友讯	
5	数字错误	CNNVD-201907-073	Qualcomm	Wind River Systems VxWorks 数字错误漏洞（CNNVD-201907-1497）
		CNNVD-201907-1497	Wind River Systems	
6	输入验证错误	CNNVD-201907-068	Qualcomm	Linksys RE6400 和 Linksys RE6300 输入验证错误漏洞（CNNVD-201907-1005）
		CNNVD-201907-079		
		CNNVD-201907-1005	Linksys	
		CNNVD-201907-1515	cPanel	
		CNNVD-201907-189	JetBrains	
		CNNVD-201907-388	微软	
		CNNVD-201907-417		
		CNNVD-201907-515	Mozilla	

		CNNVD-201907-765	Linaro	
7	授权问题	CNNVD-201907-015	Prima Systems	Cisco Vision Dynamic Signage Director 授权问题漏洞（CNNVD-201907-1030）
		CNNVD-201907-1030	思科	
		CNNVD-201907-146	摩莎	
		CNNVD-201907-180	JetBrains	
		CNNVD-201907-335	友讯	
8	权限许可和访问控制问题	CNNVD-201907-179	JetBrains	Symantec Messaging Gateway 权限许可和访问控制问题漏洞（CNNVD-201907-608）
		CNNVD-201907-203	Odoo	
		CNNVD-201907-608	Symantec	
		CNNVD-201907-653	Ivanti	
9	配置错误	CNNVD-201907-145	Cloudera	Cloudera Data Science Workbench 配置错误漏洞（CNNVD-201907-145）
		CNNVD-201907-504	Arlo Technologie	
10	命令注入	CNNVD-201907-017	Prima Systems	D-Link DIR-655 C 命令注入漏洞（CNNVD-201907-650）
		CNNVD-201907-028	NetApp	
		CNNVD-201907-619	Citrix Systems	
		CNNVD-201907-620		
		CNNVD-201907-622		
		CNNVD-201907-624		
		CNNVD-201907-650	友讯	
11	缓冲区错误	CNNVD-201708-1162	Amcrest	Microsoft Windows Server 缓冲区错误漏洞（CNNVD-201907-410）
		CNNVD-201907-152	摩莎	
		CNNVD-201907-1496	Wind River Systems	
		CNNVD-201907-1499		
		CNNVD-201907-781	Schneider Electric	
		CNNVD-201907-071	Qualcomm	
		CNNVD-201907-072		

		CNNVD-201907-077		
		CNNVD-201907-1166		
		CNNVD-201907-1332		
		CNNVD-201907-469	Mozilla	
		CNNVD-201907-488		
		CNNVD-201907-410	微软	
		CNNVD-201907-1401	Linux	
		CNNVD-201907-1402		
		CNNVD-201907-1403		
		CNNVD-201907-1407		
		CNNVD-201907-1408		
		CNNVD-201907-1409		
		CNNVD-201907-768	Linaro	
		CNNVD-201907-769		
		CNNVD-201907-770		
		CNNVD-201907-771		
		CNNVD-201907-803		
		CNNVD-201907-523	INSIDE Secure	
		CNNVD-201907-134	IBM	
12		CNNVD-201907-1147	RANGER Studio	Oracle Fusion Middleware WebLogic Server 组件访问控制错误漏洞（CNNVD-201907-924）
		CNNVD-201907-157	摩莎	
		CNNVD-201907-177	JetBrains	
		CNNVD-201907-526	Rockwell Automation	
		CNNVD-201907-777	aquaverde	
		CNNVD-201907-924	Oracle	
		CNNVD-201907-945		

		CNNVD-201907-948		
13	代码注入	CNNVD-201907-780	Schneider Electric	Schneider Electric ProClima 代码注入漏洞（CNNVD-201907-780）
14	代码问题	CNNVD-201907-214	JetBrains	MailEnable Enterprise Premium 代码问题漏洞（CNNVD-201907-378）
		CNNVD-201907-378	MailEnable	
15	安全特征问题	CNNVD-201907-196	Amcrest	Amcrest IPM-721S 安全特征问题漏洞（CNNVD-201907-196）
16	SQL 注入	CNNVD-201907-1096	Synetics	Avaya Control Manager SQL 注入漏洞（CNNVD-201907-667）
		CNNVD-201907-178	JetBrains	
		CNNVD-201907-339	友讯	
		CNNVD-201907-340		
		CNNVD-201907-554	Teclib	
		CNNVD-201907-617	Citrix Systems	
		CNNVD-201907-628	SchedMD	
		CNNVD-201907-667	Avaya	

1. Android System 组件资源管理错误漏洞（CNNVD-201907-043）

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。System 是其中的一个系统组件。

Android 9.0 版本中的 System 组件存在资源管理错误漏洞。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，补丁获取链接：

https://source.android.com/security/bulletin/2019-07-01

2. JetBrains YouTrack 插件注入漏洞（CNNVD-201907-190）

JetBrains YouTrack 是捷克 JetBrains 公司的一套基于浏览器的错误跟踪和项目管理软件。该软件具有错误跟踪、创建工作流程和监控项目进度等功能。

JetBrains YouTrack 插件（Confluence）1.8.1.3 之前版本中存在注入漏洞。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://blog.jetbrains.com/blog/2019/06/19/jetbrains-security-bulletin-q1-2019/

3. Moxa OnCell G3100-HSPA 信息泄露漏洞（CNNVD-201907-159）

Moxa OnCell G3100-HSPA 是中国台湾摩莎（Moxa）公司的一款 G3100-HSPA 系列蜂窝网络网关设备。

Moxa OnCell G3100-HSPA Series 1.6 Build 17100315 及之前版本中存在信息泄露漏洞。攻击者可利用该漏洞获取敏感信息（包括管理员密码）并可能检索其他信息，例如发送到该设备的 HTTP 请求内容或之前使用过的密码。

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.moxa.com/

4. Amcrest IPM-721S 信任管理问题漏洞（CNNVD-201907-200）

Amcrest IPM-721S 是 Amcrest 公司的一款无线 IP 摄像头。

Amcrest IPM-721S V2.420.AC00.16.R.20160909 版本中存在信任管理问题漏洞。攻击者可利用该漏洞下载管理凭证。

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://amcrest.com/

5. Wind River Systems VxWorks 数字错误漏洞（CNNVD-201907-1497）

Wind River Systems VxWorks 是美国风河系统（Wind River Systems）公司的一套嵌入式实时操作系统（RTOS）。

Wind River Systems VxWorks 中存在数字错误漏洞。攻击者可利用该漏洞执行代码。以下产品及版本受到影响：

- Wind River Systems VxWorks 6.9 版本
- Wind River Systems VxWorks 6.8 版本
- Wind River Systems VxWorks 6.7 版本
- Wind River Systems VxWorks 6.6 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.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

6. Linksys RE6400 和 Linksys RE6300 输入验证错误漏洞（CNNVD-201907-1005）

Linksys RE6400 和 Linksys RE6300 都是美国 Linksys 公司的一款无线网络信号扩展器。

Linksys RE6400 1.2.04.022 及之前版本和 RE6300 1.2.04.022 及之前版本中的 Web 界面存在输入验证错误漏洞，该漏洞源于程序没有过滤用户输入。攻击者可利用该漏洞访问系统被限制的 OS 配置及命令。

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.linksys.com/

7. Cisco Vision Dynamic Signage Director 授权问题漏洞（CNNVD-201907-1030）

Cisco Vision Dynamic Signage Director 是美国思科（Cisco）公司的一套端到端的动态标牌和 IPTV 解决方案。

Cisco Vision Dynamic Signage Director 中的 REST API 界面存在授权问题漏洞，该漏洞源于程序没有充分验证 HTTP 请求。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，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-20190717-cvdsd-wmauth

8. Symantec Messaging Gateway 权限许可和访问控制问题漏洞（CNNVD-201907-608）

Symantec Messaging Gateway 是美国赛门铁克（Symantec）公司的一套垃圾邮件过滤器。该产品具有反垃圾邮件、防病毒、高级内容过滤和数据泄露防护等功能。

Symantec Messaging Gateway 10.7.1 之前版本中存在权限许可和访问控制问题漏洞。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://support.symantec.com/us/en/article.SYMSA1486.html

9. Cloudera Data Science Workbench 配置错误漏洞（CNNVD-201907-145）

Cloudera Data Science Workbench（CDSW）是 Cloudera 公司的一套数据科学平台。该平台为企业提供快速、简易且安全的自助式数据科学支持。

Cloudera CDSW 1.3.0 及之前版本中存在配置错误漏洞。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，补丁获取链接：

https://www.cloudera.com/documentation/other/security-bulletins/topics/Security-Bulletin.html

10. D-Link DIR-655 C 命令注入漏洞（CNNVD-201907-650）

D-Link DIR-655 C 是中国台湾友讯（D-Link）公司的一款无线路由器。

D-Link DIR-655 C 3.02B05 BETA03 之前版本中存在命令注入漏洞。远程攻击者可借助‘check_fw_url’参数中的 shell 元字符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，详情请关注厂商主页：

https://www.dlink.com/

11. Microsoft Windows Server 缓冲区错误漏洞（CNNVD-201907-410）

Microsoft Windows Server 是美国微软（Microsoft）公司的一套服务器操作系统。

Microsoft Windows Server 中的 DHCP 服务存在缓冲区错误漏洞。攻击者可利用该漏洞在 DHCP 故障转移服务器上运行任意代码或者导致 DHCP 服务无法响应。以下产品及版本受到影响：

- Microsoft Windows Server 2012 版本
- Microsoft Windows Server 2012 R2 版本
- Microsoft Windows Server 2016 版本
- Microsoft Windows Server 2019 版本
- 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-2019-0785

12. Oracle Fusion Middleware WebLogic Server 组件访问控制错误漏洞（CNNVD-201907-924）

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。

Oracle Fusion Middleware 中的 WebLogic Server 组件 12.2.1.3.0 版本的 Application Container - JavaEE 子组件存在访问控制错误漏洞。攻击者可利用该漏洞控制组件，影响数据的保密性、可用性和完整性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

13. Schneider Electric ProClima 代码注入漏洞（CNNVD-201907-780）

Schneider Electric ProClima 是法国施耐德电气（Schneider Electric）公司的一套热量计算软件。该软件通过分析指定的热量数据，为控制面板内安装的环境和电气/电子设备提供热量管理功能。

Schneider Electric ProClima 8.0.0 之前版本中存在代码注入漏洞。远程攻击者可利用该漏洞在目标系统上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.schneider-electric.com/en/download/document/SEVD-2019-162-01/

14. MailEnable Enterprise Premium 代码问题漏洞（CNNVD-201907-378）

MailEnable Enterprise Premium 是澳大利亚 MailEnable 公司的一套 POP3 和 SMTP 邮件服务器。

MailEnable Enterprise Premium 10.23 版本中存在代码问题漏洞。攻击者可利用该漏洞读取主机系统上的任意文件，包括全部用户的凭证。

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/Premium-ReleaseNotes.txt

15. Amcrest IPM-721S 安全特征问题漏洞（CNNVD-201907-196）

Amcrest IPM-721S 是 Amcrest 公司的一款无线 IP 摄像头。

Amcrest IPM-721S V2.420.AC00.16.R.20160909 版本中存在安全特征问题漏洞。攻击者可利用该漏洞绕过账户保护机制并暴力破解凭证。

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://amcrest.com/

16. Avaya Control Manager SQL 注入漏洞（CNNVD-201907-667）

Avaya Control Manager 是美国 Avaya 公司的一套运营管理解决方案。该产品能够对 Avaya 产品进行统一管理。

Avaya Control Manager 7.x 版本和 8.0.4.0 之前的 8.0.x 版本中的报告组件存在 SQL 注入漏洞。远程攻击者可利用该漏洞执行任意的 SQL 命令并检索有关其他用户的敏感数据。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://downloads.avaya.com/css/P8/documents/101059368

1.4.2 高危漏洞实例

本月高危漏洞共 589 个，其中重点漏洞实例如表 6 所示。

表 6　2019 年 7 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-201907-1150	福昕	Mozilla Firefox 和 Firefox ESR 资源管理错误漏洞(CNNVD-201907-481)
		CNNVD-201907-306		
		CNNVD-201907-308		
		CNNVD-201907-310		

		CNNVD-201907-315		
		CNNVD-201907-317		
		CNNVD-201907-318		
		CNNVD-201907-327		
		CNNVD-201907-332		
		CNNVD-201907-521	Siemens	
		CNNVD-201907-801	Red Hat	
		CNNVD-201907-1321	Qualcomm	
		CNNVD-201907-1325		
		CNNVD-201907-1326		
		CNNVD-201907-1328		
		CNNVD-201907-1334		
		CNNVD-201907-481	Mozilla	
		CNNVD-201907-215	MikroTik	
		CNNVD-201907-247	Linux	
		CNNVD-201907-625	Juniper Networks	
		CNNVD-201907-1618	谷歌	
		CNNVD-201907-1643		
		CNNVD-201907-042		
		CNNVD-201907-581	思科	
		CNNVD-201907-1143	AudioCodes	
2	注入	CNNVD-201907-462	SAP	SAP Gateway 注入漏洞 (CNNVD-201907-462)
3	信息泄露	CNNVD-201907-1039	Redbrick Technologies	Oracle Fusion Middleware BI Publisher 组件信息泄露漏洞 (CNNVD-201907-909)
		CNNVD-201907-1085	Rapid7	
		CNNVD-201907-1318	Qualcomm	

		CNNVD-201907-1349	Apache	
		CNNVD-201907-1529	cPanel	
		CNNVD-201907-307	IBM	
		CNNVD-201907-333	Linux	
		CNNVD-201907-477	Mozilla	
		CNNVD-201907-502	PrestaShop	
		CNNVD-201907-600	华为	
		CNNVD-201907-603		
		CNNVD-201907-636	CloudBees	
		CNNVD-201907-721	BlackBerry	
		CNNVD-201907-796	Palo Alto Networks	
		CNNVD-201907-909	Oracle	
4	信任管理问题	CNNVD-201907-1022	思科	cPanel 信任管理问题漏洞(CNNVD-201907-1509)
		CNNVD-201907-1146	AudioCodes	
		CNNVD-201907-1509	cPanel	
		CNNVD-201907-1514		
		CNNVD-201907-165	Cloudera	
		CNNVD-201907-176	JetBrains	
		CNNVD-201907-194		
		CNNVD-201907-635	CloudBees	
		CNNVD-201907-727	Cohesity	
5	数字错误	CNNVD-201907-767	Linaro	Linaro OP-TEE 数字错误漏洞 (CNNVD-201907-767)
6	数据伪造问题	CNNVD-201907-1342	Auth0	Auth0 Passport-SharePoint 数据伪造问题漏洞 (CNNVD-201907-1342)
7	输入验证错误	CNNVD-201907-1155	福昕	F5 BIG-IP PEM 输入验证错误漏洞 (CNNVD-201907-057)
		CNNVD-201907-1156		

		CNNVD-201907-1157		
		CNNVD-201907-1159		
		CNNVD-201907-714	Zoom	
		CNNVD-201907-538	Siemens	
		CNNVD-201907-089	Quest Software	
		CNNVD-201907-066	Qualcomm	
		CNNVD-201907-070		
		CNNVD-201907-1327		
		CNNVD-201907-1138	Palo Alto Networks	
		CNNVD-201907-974	Oracle	
		CNNVD-201907-321	Odoo	
		CNNVD-201907-487	Mozilla	
		CNNVD-201907-407	微软	
		CNNVD-201907-414		
		CNNVD-201907-415		
		CNNVD-201907-423		
		CNNVD-201907-424		
		CNNVD-201907-596		
		CNNVD-201907-671	Juniper Networks	
		CNNVD-201907-204	JetBrains	
		CNNVD-201907-207		
		CNNVD-201907-208		
		CNNVD-201907-023	ImageMagick Studio	
		CNNVD-201907-024		
		CNNVD-201907-1583	IBM	
		CNNVD-201907-794	Hyland Software	

		CNNVD-201907-1259	HAProxy	
		CNNVD-201907-055	F5	
		CNNVD-201907-056		
		CNNVD-201907-057		
		CNNVD-201907-059		
		CNNVD-201907-062		
		CNNVD-201907-1508	cPanel	
		CNNVD-201907-1513		
		CNNVD-201907-1523		
		CNNVD-201907-1530		
		CNNVD-201907-1535		
		CNNVD-201907-1539		
		CNNVD-201907-221	思科	
		CNNVD-201907-234		
		CNNVD-201907-235		
		CNNVD-201907-237		
		CNNVD-201907-283	苹果	
		CNNVD-201907-685	阿帕奇	
8	授权问题	CNNVD-201907-014	Prima Systems	IBM QRadar SIEM 授权问题漏洞 (CNNVD-201907-1081)
		CNNVD-201907-032	A.T.WORKS	
		CNNVD-201907-076	Qualcomm	
		CNNVD-201907-1025	Redbrick Technologies	
		CNNVD-201907-1026		
		CNNVD-201907-1040		
		CNNVD-201907-1081	IBM	
		CNNVD-201907-1120	MongoDB	

		CNNVD-201907-163	Cloudera	
		CNNVD-201907-343	AVTECH Software	
		CNNVD-201907-369	Sonatype	
		CNNVD-201907-490	Microsoft	
		CNNVD-201907-501	ThoughtSpot	
		CNNVD-201907-514	WESEEK	
		CNNVD-201907-574	GitLab	
		CNNVD-201907-586		
		CNNVD-201907-589		
9	权限许可和访问控制问题	CNNVD-201907-074	Qualcomm	Oracle Database Server Core RDBMS 组件权限许可和访问控制问题漏洞(CNNVD-201907-839)
		CNNVD-201907-1010	ZOHO	
		CNNVD-201907-113	IBM	
		CNNVD-201907-1532	cPanel	
		CNNVD-201907-199	Amcrest	
		CNNVD-201907-228	思科	
		CNNVD-201907-231		
		CNNVD-201907-416	微软	
		CNNVD-201907-427		
		CNNVD-201907-429		
		CNNVD-201907-432		
		CNNVD-201907-433		
		CNNVD-201907-434		
		CNNVD-201907-435		
		CNNVD-201907-436		
		CNNVD-201907-437		
		CNNVD-201907-438		

		CNNVD-201907-440		
		CNNVD-201907-441		
		CNNVD-201907-450		
		CNNVD-201907-451		
		CNNVD-201907-454		
		CNNVD-201907-535	Intel	
		CNNVD-201907-692	Siemens	
		CNNVD-201907-712	Rapid7	
		CNNVD-201907-839	Oracle	
10	命令注入	CNNVD-201907-019	Prima Systems	Cisco Enterprise NFV Infrastructure Software 命令注入漏洞 (CNNVD-201907-232)
		CNNVD-201907-063	F5	
		CNNVD-201907-112	TRENDnet	
		CNNVD-201907-135		
		CNNVD-201907-136		
		CNNVD-201907-137		
		CNNVD-201907-138		
		CNNVD-201907-139		
		CNNVD-201907-140		
		CNNVD-201907-141		
		CNNVD-201907-232	思科	
		CNNVD-201907-607	Ubiquiti Networks	
		CNNVD-201907-618	Citrix Systems	
		CNNVD-201907-621		
		CNNVD-201907-800	Palo Alto Networks	
11	路径遍历	CNNVD-201907-1387	Ahsay Systems	MailEnable Enterprise Premium 路径遍历漏洞 (CNNVD-201907-373)
		CNNVD-201907-373	MailEnable	

		CNNVD-201907-826	IBM	
12	跨站请求伪造	CNNVD-201907-012	Prima Systems	IBM QRadar SIEM 跨站请求伪造漏洞 (CNNVD-201907-1193)
		CNNVD-201907-1064	AudioCodes	
		CNNVD-201907-1193	IBM	
		CNNVD-201907-148	摩莎	
		CNNVD-201907-166	Open-Xchange	
		CNNVD-201907-181	Rapid7	
		CNNVD-201907-187	JetBrains	
		CNNVD-201907-480	Mozilla	
		CNNVD-201907-629	CloudBees	
		CNNVD-201907-997		
		CNNVD-201907-652	友讯	
13	跨站脚本	CNNVD-201907-048	F5	F5 BIG-IP 跨站脚本漏洞 (CNNVD-201907-048)
		CNNVD-201907-246	Stormshield	
14	竞争条件问题	CNNVD-201907-1336	Qualcomm	多款 Qualcomm 产品竞争条件问题漏洞 (CNNVD-201907-1336)
		CNNVD-201907-1493	Wind River Systems	
15	加密问题	CNNVD-201907-168	DNN	JetBrains Kotlin 加密问题漏洞 (CNNVD-201907-202)
		CNNVD-201907-169		
		CNNVD-201907-171		
		CNNVD-201907-173		
		CNNVD-201907-202	JetBrains	
16	缓冲区错误	CNNVD-201907-034	谷歌	Android 缓冲区错误漏洞 (CNNVD-201907-034)
		CNNVD-201907-035		
		CNNVD-201907-036		
		CNNVD-201907-040		
		CNNVD-201907-091		

		CNNVD-201907-1137	IBM	
		CNNVD-201907-1152	福昕	
		CNNVD-201907-069	Qualcomm	
		CNNVD-201907-083		
		CNNVD-201907-086		
		CNNVD-201907-1164		
		CNNVD-201907-1322		
		CNNVD-201907-1323		
		CNNVD-201907-1324		
		CNNVD-201907-1329		
		CNNVD-201907-1330		
		CNNVD-201907-1331		
		CNNVD-201907-1494	Wind River Systems	
		CNNVD-201907-1498	Wind River Systems	
		CNNVD-201907-153	摩莎	
		CNNVD-201907-1626	友讯	
		CNNVD-201907-1598	思科	
		CNNVD-201907-229		
		CNNVD-201907-236		
		CNNVD-201907-280	Artifex Software	
		CNNVD-201907-285	ImageMagick Studio	
		CNNVD-201907-286		
		CNNVD-201907-288		
		CNNVD-201907-289		
		CNNVD-201907-290		
		CNNVD-201907-291		

		CNNVD-201907-292		
		CNNVD-201907-295		
		CNNVD-201907-298		
		CNNVD-201907-299		
		CNNVD-201907-300		
		CNNVD-201907-302		
		CNNVD-201907-344		
		CNNVD-201907-389	微软	
		CNNVD-201907-390		
		CNNVD-201907-391		
		CNNVD-201907-392		
		CNNVD-201907-393		
		CNNVD-201907-398		
		CNNVD-201907-400		
		CNNVD-201907-401		
		CNNVD-201907-403		
		CNNVD-201907-406		
		CNNVD-201907-409		
		CNNVD-201907-425		
		CNNVD-201907-428		
		CNNVD-201907-442		
		CNNVD-201907-443		
		CNNVD-201907-444		
		CNNVD-201907-445		
		CNNVD-201907-446		
		CNNVD-201907-447		
		CNNVD-201907-448		

		CNNVD-201907-449		
		CNNVD-201907-484		
		CNNVD-201907-562	Redis Labs	
		CNNVD-201907-660		
		CNNVD-201907-672	Juniper Networks	
		CNNVD-201907-688		
		CNNVD-201907-693	台达电子	
17	访问控制错误	CNNVD-201907-1002	Temenos	Oracle Food and Beverage Applications Hospitality Simphony 组件访问控制错误漏洞 (CNNVD-201907-1043)
		CNNVD-201907-1127	Code42 Software	
		CNNVD-201907-1140	HPE	
		CNNVD-201907-1304	McAfee	
		CNNVD-201907-197	Odoo	
		CNNVD-201907-201		
		CNNVD-201907-371	MailEnable	
		CNNVD-201907-464	SAP	
		CNNVD-201907-580	GitLab	
		CNNVD-201907-632	Cloudera	
		CNNVD-201907-669	博文教育	
		CNNVD-201907-818	联想	
		CNNVD-201907-1043	Oracle	
		CNNVD-201907-1044		
		CNNVD-201907-836		
		CNNVD-201907-843		
		CNNVD-201907-844		
		CNNVD-201907-845		
		CNNVD-201907-846		
		CNNVD-201907-847		

		CNNVD-201907-848		
		CNNVD-201907-855		
		CNNVD-201907-856		
		CNNVD-201907-863		
		CNNVD-201907-867		
		CNNVD-201907-870		
		CNNVD-201907-872		
		CNNVD-201907-876		
		CNNVD-201907-881		
		CNNVD-201907-885		
		CNNVD-201907-887		
		CNNVD-201907-896		
		CNNVD-201907-908		
		CNNVD-201907-910		
		CNNVD-201907-925		
		CNNVD-201907-926		
		CNNVD-201907-927		
		CNNVD-201907-928		
		CNNVD-201907-929		
		CNNVD-201907-930		
		CNNVD-201907-932		
		CNNVD-201907-933		
		CNNVD-201907-936		
		CNNVD-201907-937		
		CNNVD-201907-938		
		CNNVD-201907-939		
		CNNVD-201907-940		

		CNNVD-201907-941		
		CNNVD-201907-942		
		CNNVD-201907-943		
		CNNVD-201907-944		
		CNNVD-201907-946		
		CNNVD-201907-947		
		CNNVD-201907-952		
		CNNVD-201907-955		
		CNNVD-201907-957		
		CNNVD-201907-958		
		CNNVD-201907-959		
		CNNVD-201907-961		
		CNNVD-201907-982		
18	代码问题	CNNVD-201907-067	Qualcomm	Adobe Dreamweaver direct download installer 代码问题漏洞 (CNNVD-201907-525)
		CNNVD-201907-1165		
		CNNVD-201907-1112	RANGER Studio	
		CNNVD-201907-1114		
		CNNVD-201907-1136		
		CNNVD-201907-1153	福昕	
		CNNVD-201907-1154		
		CNNVD-201907-1158		
		CNNVD-201907-1282	MODX	
		CNNVD-201907-1283	Mitsubishi Electric	
		CNNVD-201907-1381	IBM	
		CNNVD-201907-1386	Ahsay Systems	
		CNNVD-201907-1359		
		CNNVD-201907-155	摩莎	

		CNNVD-201907-1622	阿帕奇	
		CNNVD-201907-226	思科	
		CNNVD-201907-361	GitLab	
		CNNVD-201907-582		
		CNNVD-201907-413	微软	
		CNNVD-201907-426		
		CNNVD-201907-459	SAP	
		CNNVD-201907-525	Adobe	
		CNNVD-201907-516	Siemens	
		CNNVD-201907-609		
		CNNVD-201907-782	Schneider Electric	
19	操作系统命令注入	CNNVD-201907-457	SAP	SAP Diagnostics Agent 操作系统命令注入漏洞 (CNNVD-201907-458)
		CNNVD-201907-458		
20	参数注入	CNNVD-201907-1490	Wind River Systems	Wind River Systems VxWorks 参数注入漏洞 (CNNVD-201907-1495)
		CNNVD-201907-1491		
		CNNVD-201907-1495		
21	SQL 注入	CNNVD-201907-1108	Elcom Technology	Elcom Technology Elcom CMS SQL 注入漏洞 (CNNVD-201907-1108)
		CNNVD-201907-798	SolarWinds Network	

1. Mozilla Firefox 和 Firefox ESR 资源管理错误漏洞（CNNVD-201907-481）

Mozilla Firefox 和 Mozilla Firefox ESR 都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。

Mozilla Firefox 68 之前版本和 Firefox ESR 60.8 之前版本中存在资

源管理错误漏洞。攻击者可利用该漏洞造成拒绝服务（浏览器崩溃）。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/

2. SAP Gateway 注入漏洞(CNNVD-201907-462)

SAP Gateway 是德国思爱普（SAP）公司的一款基于开放标准的框架。该产品支持非 SAP 应用程序连接到 SAP 应用程序，还可连接和访问移动设备上的 SAP 应用程序。

SAP Gateway 中存在注入漏洞，该漏洞源于程序没有正确过滤用户提交的输入。攻击者可利用该漏洞注入内容，进而使用户相信该内容来自合法服务。以下产品及版本受到影响：

- SAP Gateway 7.5 版本
- SAP Gateway 7.51 版本
- SAP Gateway 7.52 版本
- SAP Gateway 7.53 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://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=523994575

3. Oracle Fusion Middleware BI Publisher 组件信息泄露漏洞(CNNVD-201907-909)

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提

供了中间件、软件集合等功能。BI Publisher（前称 XML Publisher）是其中的一个报表组件。

Oracle Fusion Middleware 中的 BI Publisher (formerly XML Publisher)组件 11.1.1.9.0 版本的 BI Publisher Security 子组件存在信息泄露漏洞。攻击者可利用该漏洞未授权访问数据，影响数据的保密性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

4. cPanel 信任管理问题漏洞(CNNVD-201907-1509)

cPanel 是美国 cPanel 公司的一套基于 Web 的自动化主机托管平台。该平台主要用于自动化管理网站和服务器。

cPanel 82.0.2 之前版本中存在信任管理问题漏洞。本地攻击者可利用该漏洞获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://documentation.cpanel.net/display/CL/82+Change+Log

5. Linaro OP-TEE 数字错误漏洞(CNNVD-201907-767)

Linaro OP-TEE 是英国 Linaro 公司的一套开源的可信任执行环境。

Linaro OP-TEE 3.3.0 及之前版本中的 optee_os 存在数字错误漏洞。攻击者可利用该漏洞泄露之前 Trusted Application 中的密码和/或数据。

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/OP-TEE/optee_os/commit/7e768f8a473409215fe3fff8f6e31f8a3a0103c6

6. Auth0 Passport-SharePoint 数据伪造问题漏洞（CNNVD-201907-1342）

Auth0 Passport-SharePoint 是美国 Auth0 公司的一款使用 SharePoint 帐户对用户进行身份验证软件包。

Auth0 Passport-SharePoint 0.4.0 之前版本中存在数据伪造问漏洞，该漏洞源于程序在处理访问令牌之前没有验证 JWT 签名。攻击者可利用该漏洞伪造令牌并绕过身份验证及授权机制。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://auth0.com/docs/security/bulletins/cve-2019-13483

7. F5 BIG-IP PEM 输入验证错误漏洞（CNNVD-201907-057）

F5 BIG-IP PEM 是美国 F5 公司的使用在 BIG-IP 中的一款策略执行器。

F5 BIG-IP PEM 14.1.0 版本至 14.1.0.5 版本和 14.0.0 版本至 14.0.0.4 版本中存在输入验证错误漏洞。攻击者可利用该漏洞造成 TMM 进程终止并重启。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.f5.com/csp/article/K04730051

8. IBM QRadar SIEM 授权问题漏洞（CNNVD-201907-1081）

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。

IBM QRadar SIEM 7.2 版本和 7.3 版本中的日志文件协议存在授权

问题漏洞。攻击者可利用该漏洞读取或修改资源。

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=ibm10958889

9. **Oracle Database Server Core RDBMS 组件权限许可和访问控制问题漏洞(CNNVD-201907-839)**

Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。Core RDBMS 是其中的一个关系型数据库核心组件。

Oracle Database Server 中的 Core RDBMS 组件存在权限许可和访问控制问题漏洞。攻击者可利用该漏洞未授权访问、更新、插入或删除数据，影响数据的保密性和完整性。以下产品及版本受到影响：

- Oracle Database Server 12.1.0.2 版本
- Oracle Database Server 12.2.0.1 版本
- Oracle Database Server 18c 版本
- Oracle Database Server 19c 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.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

10. **Cisco Enterprise NFV Infrastructure Software 命令注入漏洞(CNNVD-201907-232)**

Cisco Enterprise NFV Infrastructure Software（NFVIS）是美国思科（Cisco）公司的一套 NVF 基础架构软件平台。该平台可以通过中央

协调器和控制器实现虚拟化服务的全生命周期管理。

Cisco Enterprise NFVIS 3.10.1 之前版本中存在命令注入漏洞，该漏洞源于程序没有进行充分的输入验证。本地攻击者可借助恶意的输入利用该漏洞在底层操作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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-commandinj

11. MailEnable Enterprise Premium 路径遍历漏洞(CNNVD-201907-373)

MailEnable Enterprise Premium 是澳大利亚 MailEnable 公司的一套 POP3 和 SMTP 邮件服务器。

MailEnable Enterprise Premium 10.23 版本中存在路径遍历漏洞。攻击者可利用该漏洞添加、移除或读取 IIS 用户可访问的任意文件夹中的文件，读取其他用户的凭证（包括 SYSADMIN 账户），读取其他用户的邮件或向其他用户账户添加邮件或文件。

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/Premium-ReleaseNotes.txt

12. IBM QRadar SIEM 跨站请求伪造漏洞(CNNVD-201907-1193)

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。

IBM QRadar SIEM 中存在跨站请求伪造漏洞。远程攻击者可利用

该漏洞执行恶意的操作。以下产品及版本受到影响：

- IBM QRadar 7.3 版本至 7.3.2 Patch 1
- IBM QRadar 7.2 版本至 7.2.8 Patch 15 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-01.ibm.com/support/docview.wss?uid=ibm10959463

13. F5 BIG-IP 跨站脚本漏洞(CNNVD-201907-048)

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。

F5 BIG-IP（AFM 和 ASM）中的 AFM feed 列表存在跨站脚本漏洞，该漏洞源于程序没有充分过滤用户提交的输入。远程攻击者可利用该漏洞在受影响网站的上下文中执行 HTML 或 JavaScript 代码。以下产品及版本受到影响：

- F5 BIG-IP 14.1.0 版本至 14.1.0.5 版本
- F5 BIG-IP 14.0.0 版本至 14.0.0.4 版本
- F5 BIG-IP 13.0.0 版本至 13.1.1.4 版本
- F5 BIG-IP 12.1.0 版本至 12.1.4 版本
- F5 BIG-IP 11.5.1 版本至 11.6.4 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://support.f5.com/csp/article/K68151373

14. 多款 Qualcomm 产品竞争条件问题漏洞(CNNVD-201907-1336)

Qualcomm MSM8996AU 等都是美国高通（Qualcomm）公司的产品。MSM8996AU 是一款中央处理器（CPU）产品。SD 712 是一款

中央处理器（CPU）产品。SDX24 是一款调制解调器。

多款 Qualcomm 产品中的 Camera 库存在竞争条件问题漏洞，该漏洞源于网络系统或产品在运行过程中，并发代码需要互斥地访问共享资源时，对于并发访问的处理不当。以下产品及版本受到影响：

- Qualcomm MSM8909W
- Qualcomm MSM8996AU
- Qualcomm QCS605
- Qualcomm SD 425
- Qualcomm SD 427
- Qualcomm SD 430
- Qualcomm SD 435
- Qualcomm SD 450
- Qualcomm SD 625
- Qualcomm SD 636
- Qualcomm SD 712
- Qualcomm SD 710
- Qualcomm SD 670
- Qualcomm SD 820
- Qualcomm SD 820A
- Qualcomm SD 835
- Qualcomm SD 845
- Qualcomm SD 850

- Qualcomm SDA660
- Qualcomm SDM660
- Qualcomm SDX20
- Qualcomm SDX24

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.qualcomm.com/

15. JetBrains Kotlin 加密问题漏洞(CNNVD-201907-202)

JetBrains Kotlin 是捷克 JetBrains 公司的一款在 Java 虚拟机上运行的静态类型编程语言。

JetBrains Kotlin 1.3.30 之前版本中存在加密问题漏洞。攻击者可利用该漏洞实施中间人攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://blog.jetbrains.com/blog/2019/06/19/jetbrains-security-bulletin-q1-2019/

16. Android 缓冲区错误漏洞(CNNVD-201907-034)

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。

Android 中的 AVIExtractor.cpp 文件的 MakeMPEG4VideoCodecSpecificData 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。以下产品及版本受到影响：

- Android 7.0 版本
- Android 7.1.1 版本

- Android 7.1.2 版本
- Android 8.0 版本
- Android 8.1 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://source.android.com/security/bulletin/2019-07-01

17. Oracle Food and Beverage Applications Hospitality Simphony 组件访问控制错误漏洞(CNNVD-201907-1043)

Oracle Food and Beverage Applications 是美国甲骨文（Oracle）公司的一套餐饮销售管理解决方案。Hospitality Simphony 是其中的一个基于云的移动餐饮销售组件。

Oracle Food and Beverage Applications 中的 Hospitality Simphony 组件 18.2.1 版本存在访问控制错误漏洞。攻击者可利用该漏洞未授权访问数据，影响数据的保密性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

18. Adobe Dreamweaver direct download installer 代码问题漏洞(CNNVD-201907-525)

Adobe Dreamweaver 是美国奥多比（Adobe）公司的一款支持可视化 HTML 编辑和代码编辑的软件。Adobe Dreamweaver direct download installer 是一款 Adobe Dreamweaver 的安装程序。。

基于 Windows 平台的 Adobe Dreamweaver direct download installer

18.0 及之前版本和 19.0 及之前版本中存在代码问题漏洞。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://helpx.adobe.com/security/products/dreamweaver/apsb19-40.html

19. SAP Diagnostics Agent 操作系统命令注入漏洞

(CNNVD-201907-458)

SAP Diagnostics Agent 是德国思爱普（SAP）公司的一款系统诊断代理程序。

SAP Diagnostic Agent (LM-Service) 7.2 版本中存在操作系统命令注入漏洞。攻击者可利用该漏洞注入代码，控制应用程序的运行。

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=523994575

20. Wind River Systems VxWorks 参数注入漏洞

(CNNVD-201907-1495)

Wind River Systems VxWorks 是美国风河系统（Wind River Systems）公司的一套嵌入式实时操作系统（RTOS）。

Wind River Systems VxWorks 中存在参数注入漏洞。攻击者可借助畸形的 TCP 选项利用该漏洞造成拒绝服务。以下产品及版本受到影响：

- Wind River Systems VxWorks 7 版本

- Wind River Systems VxWorks 6.9 版本
- Wind River Systems VxWorks 6.8 版本
- Wind River Systems VxWorks 6.7 版本
- Wind River Systems VxWorks 6.6 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.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

21. Elcom Technology Elcom CMS SQL 注入漏洞

(CNNVD-201907-1108)

Elcom Technology Elcom CMS 是澳大利亚 Elcom Technology 公司的一套基于 ASP.NET 和 SQL Server 的 Web 内容管理系统（CMS）。

Elcom Technology Elcom CMS 10.7 之前版本中存在 SQL 注入漏洞。远程攻击者可利用该漏洞获取敏感信息。

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.elcom.com.au/

二、接报漏洞情况

本月接报漏洞共计 7982 个，其中信息技术产品漏洞（通用型漏洞）96 个，网络信息系统漏洞（事件型漏洞）7886 个。

表 7 2018 年 7 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	5900	0	5900

2	网神信息技术（北京）股份有限公司	1389	0	1389
3	中新网络信息安全股份有限公司	246	0	246
4	山东新潮信息技术有限公司	146	0	146
5	北京数字观星科技有限公司	74	0	74
6	内蒙古奥创科技有限公司	55	1	54
7	北京圣溥润高新技术服份有限公司	27	0	27
8	网神信息技术（北京）股份有限公司奇安信代码安全实验室	24	24	0
9	广州锦行网络科技有限公司	21	1	20
10	国发中新（北京）科技发展有限公司	14	0	14
11	杭州海康威视数字技术股份有限公司	13	0	13
12	北京天融信网络安全技术有限公司	11	11	0
13	厦门服云信息科技有限公司	7	7	0
14	中兴通讯股份有限公司	6	6	0
15	四川师范大学	6	6	0
16	杭州安恒信息技术股份有限公司	5	5	0
17	北京神州绿盟科技有限公司安全研究部	5	5	0
18	广州竞远安全技术股份有限公司	4	4	0
19	清华大学网络科学与网络空间研究院	3	3	0
20	北京梆梆安全科技有限公司	3	3	0
21	亚信科技（成都）有限公司	3	3	0
22	广州万方计算机科技有限公司	3	3	0

23	江苏博智软件科技股份有限公司	2	2	0
24	北京山石网科信息技术有限公司	2	2	0
25	上海安识网络科技有限公司	2	0	2
26	福建经联网络技术有限公司	2	2	0
27	个人	2	1	1
28	北京启明星辰信息安全技术有限公司西安分公司	1	1	0
29	北京国舜科技股份有限公司	1	1	0
30	杭州汉领信息科技有限公司汉武安全实验室	1	1	0
31	北京未来安全信息技术有限公司	1	1	0
32	北京威努特技术有限公司	1	1	0
33	北京安华金和科技有限公司	1	1	0
34	北京长亭科技有限公司	1	1	0
报送总计		7982	96	7886

三、重大漏洞预警

3.1 关于 Fastjson 远程代码执行漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Fastjson 远程代码执行漏洞（CNNVD-201907-699）情况的报送，此漏洞为 2017 年 Fastjson 1.2.24 版本反序列化漏洞的延伸利用。攻击者可以通过发送精心构造的请求包在使用 Fastjson 的服务器上远程执行恶意代码。Fastjson1.2.51 以下版本均受漏洞影响。目前，厂商未发表声明，但可通过升级 Fastjson 到最新版本修补漏洞带来的危害，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

Fastjson 是一个 Java 语言编写的 JSON 库。Fastjson 存在远程代码执行漏洞（CNNVD-201907-699），当应用或系统使用 Fastjson 对由用户可控的 JSON 字符串数据进行解析时，可触发远程代码执行漏洞。该漏洞为 2017 年 Fastjson 1.2.24 版本反序列化漏洞的延伸利用。攻击者可以通过发送精心构造的请求包在使用 Fastjson 的服务器上远程执行恶意代码。

漏洞危害

成功利用该漏洞的攻击者在使用 Fastjson 的服务器上远程执行恶意代码。Fastjson1.2.51 以下版本均受漏洞影响

修复措施

目前，厂商未发表声明，但可通过升级 Fastjson 到最新版本 1.2.58 修补漏洞带来的危害，具体方法如下：

https://github.com/alibaba/fastjson/wiki/update_faq_20190722

3.2 关于 VxWorks 多个远程代码执行漏洞情况的通报

近日，VxWorks 官方发布了多个安全漏洞公告，包括 VxWorks 缓冲区错误漏洞（CNNVD-201907-1499 、CVE-2019-12256）、VxWorks 安全漏洞（CNNVD-201907-1497 、CVE-2019-12255）等多个漏洞。VxWorks 7、VxWorks 6.5-6.9 及使用 Interpeak 独立网络堆栈的 VxWorks 版本均受漏洞影响。成功利用上述漏洞的攻击者无需用户交互及认证即可实现远程代码攻击，最终完全控制相关设备。目前，VxWorks 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，尽快采取修补措施。

漏洞简介

VxWorks 是一种在嵌入式系统中部署的实时操作系统，是由美国 WindRiver 公司（简称风河公司，即 WRS 公司）于 1983 年设计开发的，VxWorks 被超过 20 亿台设备使用，包括关键基础设施、网络设备、医疗设备、工业系统、甚至航天器。该系统从 PLC 到 MRI 机器、防火墙、打印机、再到飞机和火车等都有广泛应用。

1、VxWorks 缓冲区错误漏洞（CNNVD-201907-1499 、CVE-2019-12256）：

当攻击者向受此漏洞影响的 VxWorks 设备发送包含多个 Source Record Route（SRR）option 的畸形 IP 数据包时，目标设备将会生成 ICMP 错误数据包作为响应，并且在不经安全验证的情况下将攻击者的畸形 IP 数据包复制到响应数据包的 IP 选项中，最终导致出现堆栈溢出。

2、VxWorks 安全漏洞（CNNVD-201907-1497 、CVE-2019-12255）（CNNVD-201907-1496、CVE-2019-12260）（CNNVD-201907-1494、CVE-2019-12261）（CNNVD-201907-1493、CVE-2019-12263）：

TCP 有一种机制来传输名为“紧急数据”的越界数据。通过利用这种机制，攻击者可以使传入 recv()系统调用的 length 变量下溢，这将导致传入 recv()系统调用的缓冲区出现攻击者可控的溢出，最终导致远程代码执行。

3、VxWorksDHCP 客户端堆溢出漏洞（CNNVD-201907-1498、CVE-2019-12257）：

VxWorks DHCP 客户端在解析 DHCP 服务器发回的 DHCP Offer 与 ACK 数据包时存在堆溢出漏洞。当攻击者与目标设备处于同一网络时，且当目标设备发送了 DHCPDiscovery 数据包后，攻击者可通过向目标设备发送一个精心构造的 DHCP Offer 数据包来触发此堆溢

出漏洞。攻击者可通过此漏洞在目标设备执行任意代码。

漏洞危害

成功利用上述漏洞的攻击者无需用户交互及认证即可实现远程代码攻击，最终完全控制相关设备。VxWorks 7、VxWorks 6.5-6.9 及使用 Interpeak 独立网络堆栈的 VxWorks 版本均受漏洞影响。具体如下：

	漏洞编号	影响范围
1	VxWorks 安全漏洞（CNNVD-201907-1497 、CVE-2019-12255）（CNNVD-201907-1496、CVE-2019-12260）（CNNVD-201907-1494、CVE-2019-12261）（CNNVD-201907-1493、CVE-2019-12263）	VxWorks 6.6、VxWorks 6.7、VxWorks 6.8、VxWorks 6.9、VxWorks 7
2	VxWorks 缓冲区错误漏洞（CNNVD-201907-1499 、CVE-2019-12256）	VxWorks 6.9、VxWorks 7
3	VxWorksDHCP 客户端堆溢出漏洞（CNNVD-201907-1498、CVE-2019-12257）	VxWorks 6.6、VxWorks 6.7、VxWorks 6.8、VxWorks 6.9

安全建议

目前，VxWorks 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。官方链接如下：

https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/