北京师范大学网络信息安全通告

2019 年 8 月报告

北京师范大学信息网络中心

2019 年 9 月

目录

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 8 月份新增安全漏洞共 2264 个，从厂商分布来看，Google 公司产品的漏洞数量最多，共发布 289 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 19.26%。本月新增漏洞中，超危漏洞 233 个、高危漏洞 576 个、中危漏洞 1420 个、低危漏洞 35 个，相应修复率分别为 87.12%、84.90%、85.28%以及 80.00%。合计 1931 个漏洞已有修复补丁发布，本月整体修复率 85.29%。

截至 2019 年 8 月 31 日，CNNVD 采集漏洞总量已达 131803 个。

1.1 漏洞增长概况

2019 年 8 月新增安全漏洞 2264 个，与上月（1670 个）相比增加了 35.57%。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 1549 个。

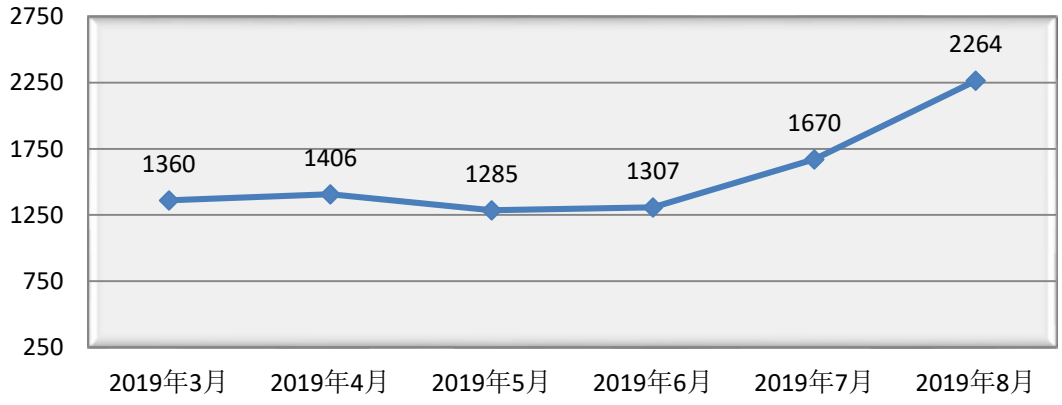

图 1 2019 年 3 月至 2019 年 8 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

8 月厂商漏洞数量分布情况如表 1 所示，Google 公司达到 289 个，占本月漏洞总量的 12.77%。本月谷歌、Adobe 等公司的漏洞数量均有所上升。

表 1　2019 年 8 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	谷歌	289	12.77%
2	cPanel	277	12.23%
3	Adobe	117	5.17%
4	微软	88	3.89%
5	思科	73	3.22%
6	IBM	46	2.03%
7	Linux	43	1.90%
8	Magento	30	1.33%
9	CloudBees	24	1.06%
10	SAP	19	0.84%

1.2.2 漏洞产品分布

8 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 65 条，其中桌面操作系统 62 条，服务器操作系统 64 条。本月 Android 漏洞数量最多，共 276 个，占主流操作系统漏洞总量的 38.66%，排名第一。

表 2　2019 年 8 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	Android	276
2	Windows 10	59

3	Windows Server 版本 1903	57
4	Windows Server 版本 1803	54
5	Windows Server 2016	43
6	Linux Kernel	42
7	Windows Server 2012	38
8	Windows Server 2008	38
9	Windows 7	37
10	Windows 8.1	37
11	Windows Rt 8.1	33

*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

8 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 19.26%。

表 32019 年 8 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	436	19.26%
2	信息泄露	237	10.47%
3	缓冲区错误	236	10.42%
4	输入验证错误	190	8.39%
5	跨站请求伪造	102	4.51%
6	代码问题	96	4.24%
7	SQL 注入	95	4.20%
8	权限许可和访问控制问题	92	4.06%

9	资源管理错误	91	4.02%
10	授权问题	78	3.45%
11	访问控制错误	64	2.83%
12	安全特征问题	42	1.86%
13	路径遍历	42	1.86%
14	命令注入	31	1.37%
15	信任管理问题	30	1.33%
16	注入	27	1.19%
17	加密问题	15	0.66%
18	操作系统命令注入	15	0.66%
19	日志信息泄露	13	0.57%
20	代码注入	13	0.57%
21	数字错误	11	0.49%
22	数据伪造问题	3	0.13%
23	格式化字符串错误	3	0.13%
24	竞争条件问题	3	0.13%
25	配置问题	1	0.04%
26	参数注入	1	0.04%
27	后置链接	1	0.04%

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。8 月漏洞危害等级分布如图 2 所示，其中超危漏洞 233 条，占本月漏洞总数的 10.29%。

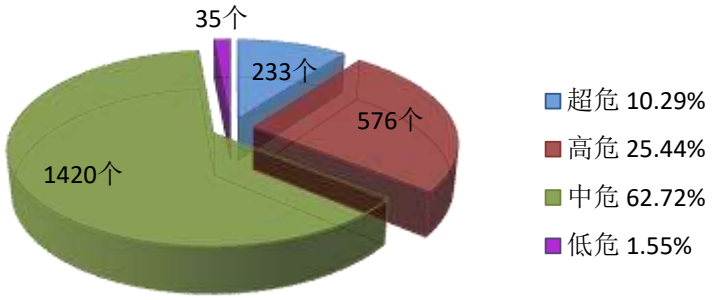

图 2　2019 年 8 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

8 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 87.12%，低高危漏洞修复率最低，比例为 80.00%。与上月相比，本月超、高、中、低危漏洞修复率有所上升。总体来看，本月整体修复率上升，由上月的 77.19%上升至本月的 85.29%。

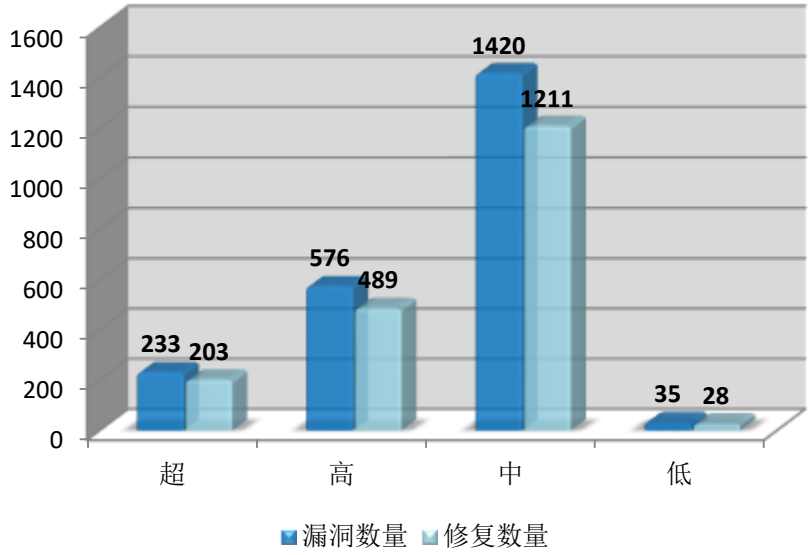

图 3　2019 年 8 月漏洞修复数量统计

1.3.2 厂商修复情况

8 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Google、cPanel、Adobe 等十个厂商共 1006 条漏洞，占本月漏洞总数的 44.43%，漏洞修复率为 89.96%，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 cPanel、Adobe、Microsoft、IBM 等公司本月漏洞修复率均为 100%，共 748 条漏洞已全部修复。

表 4　2019 年 8 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	Google	289	215	74.39%
2	cPanel	277	277	100.00%
3	Adobe	117	117	100.00%
4	Microsoft	88	88	100.00%
5	Cisco	73	69	94.52%
6	IBM	46	46	100.00%
7	Linux	43	39	90.70%
8	Magento	30	30	100.00%
9	CloudBees	24	7	29.17%
10	SAP	19	17	89.47%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 233 个，其中重要漏洞实例如表 5 所示。

表 5　2019 年 8 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-201908-1571	Linux	Adobe Acrobat 和

		CNNVD-201908-496	Linux	Reader 资源管理错误漏洞 (CNNVD-201908-726)
		CNNVD-201908-726	Adobe	
		CNNVD-201908-748		
		CNNVD-201908-750		
		CNNVD-201908-751		
		CNNVD-201908-752		
		CNNVD-201908-753		
		CNNVD-201908-755		
		CNNVD-201908-758		
		CNNVD-201908-765		
		CNNVD-201908-777		
		CNNVD-201908-782		
		CNNVD-201908-792		
		CNNVD-201908-836		
2	信任管理问题	CNNVD-201908-1138	Johnson Controls	Johnson Controls Metasys system 信任管理问题漏洞 (CNNVD-201908-1138)
		CNNVD-201908-1153		
		CNNVD-201908-1721	Cisco	
3	输入验证错误	CNNVD-201908-1857	Palo Alto Networks	Palo Alto Networks PAN-OS 输入验证错误漏洞 (CNNVD-201908-1857)
		CNNVD-201908-1931	Fortinet	
		CNNVD-201908-2165	Lexmark	
		CNNVD-201908-720	Adobe	
		CNNVD-201908-912	eQ-3	
		CNNVD-201908-923	Google	
4	授权问题	CNNVD-201908-1064	Micro Focus	Cisco Small Business 220 Series Smart Switches 授权问题漏洞 (CNNVD-201908-422
		CNNVD-201908-1723	Cisco	
		CNNVD-201908-1725		

		CNNVD-201908-1726		)
		CNNVD-201908-2149		
		CNNVD-201908-422		
		CNNVD-201908-623	HPE	
		CNNVD-201908-627		
		CNNVD-201908-630		
		CNNVD-201908-799	Adobe	
5	权限许可和访问控制问题	CNNVD-201908-722	Adobe	Adobe Creative Cloud Desktop Application 权限许可和访问控制问题漏洞 (CNNVD-201908-722)
6	命令注入	CNNVD-201908-1079	普联	Adobe Photoshop CC 命令注入漏洞 (CNNVD-201908-800)
		CNNVD-201908-783	Adobe	
		CNNVD-201908-800		
7	加密问题	CNNVD-201908-353	NetApp	NetApp Clustered Data ONTAP 加密问题漏洞 (CNNVD-201908-353)
8	缓冲区错误	CNNVD-201908-1005	Microsoft	Microsoft Windows DHCP 客户端缓冲区错误漏洞 (CNNVD-201908-1005)
		CNNVD-201908-968		
		CNNVD-201908-1942	Delta Controls	
		CNNVD-201908-2167	Lexmark	
		CNNVD-201908-2168		
		CNNVD-201908-2214	ROBOTIS	
		CNNVD-201908-309	NVIDIA	
		CNNVD-201908-369		
		CNNVD-201908-426	Cisco	
		CNNVD-201908-433	Qualcomm	
		CNNVD-201908-434		

		CNNVD-201908-732	Adobe	
		CNNVD-201908-737		
		CNNVD-201908-740		
		CNNVD-201908-741		
		CNNVD-201908-746		
		CNNVD-201908-749		
		CNNVD-201908-762		
		CNNVD-201908-764		
		CNNVD-201908-770		
		CNNVD-201908-771		
		CNNVD-201908-772		
		CNNVD-201908-786		
		CNNVD-201908-789		
		CNNVD-201908-790		
		CNNVD-201908-821		
		CNNVD-201908-825		
		CNNVD-201908-826		
		CNNVD-201908-853		
		CNNVD-201908-862		
		CNNVD-201908-870		
		CNNVD-201908-1855	Palo Alto Networks	
9	访问控制错误	CNNVD-201908-1089	eQ-3	eQ-3 HomeMatic CCU2 和 eQ-3 Homematic CCU3 访问控制错误漏洞 (CNNVD-201908-1090)
		CNNVD-201908-1090		
		CNNVD-201908-161	3S-Smart Software Solutions	
		CNNVD-201908-207	Siemens	
		CNNVD-201908-2129	Lexmark	

		CNNVD-201908-491	Cisco	
		CNNVD-201908-702	HashiCorp	
		CNNVD-201908-953	Microsoft	
		CNNVD-201908-955		
		CNNVD-201908-962		
		CNNVD-201908-964		
10	代码问题	CNNVD-201908-399	Google	Android 代码问题漏洞 (CNNVD-201908-399)
		CNNVD-201908-581	ZOHO	
		CNNVD-201908-729	Adobe	
		CNNVD-201908-744		
		CNNVD-201908-768		
		CNNVD-201908-801		
		CNNVD-201908-802		
		CNNVD-201908-803		
		CNNVD-201908-804		
		CNNVD-201908-805		
		CNNVD-201908-806		
		CNNVD-201908-807		
		CNNVD-201908-894	SAP	
11	操作系统命令注入	CNNVD-201908-558	Cisco	Cisco Enterprise NFV Infrastructure Software 操作系统命令注入漏洞 (CNNVD-201908-558)
12	安全特征问题	CNNVD-201908-624	HPE	HPE 3PAR Service Processor 安全特征问题漏洞 (CNNVD-201908-624)
13	SQL 注入	CNNVD-201908-1234	IBM	IBM Emptoris Contract Management SQL 注入漏洞
		CNNVD-201908-1235		

		CNNVD-201908-1970	Alfresco Software	(CNNVD-201908-1234)
		CNNVD-201908-016	cPanel	

1. Adobe Acrobat 和 Reader 资源管理错误漏洞(CNNVD-201908-726)

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。

Adobe Acrobat 和 Acrobat Reader 中存在资源管理错误漏洞。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：

- 基于 macOS 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Continuous ）2019.012.20034 及之前版本
- 基于 Windows 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Continuous ）2019.012.20035 及之前版本
- 基于 macOS 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Classic 2017 ）2017.011.30142 及之前版本
- 基于 Windows 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Classic 2017 ）2017.011.30143 及之前版本
- 基于 macOS 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Classic 2015 ）2015.006.30497 及之前版本
- 基于 Windows 平台的 Adobe Acrobat DC 和 Acrobat Reader DC（Classic 2015）2015.006.30498 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/acrobat/apsb19-41.html

2. Johnson Controls Metasys system 信任管理问题漏洞（CNNVD-201908-1138）

Johnson Controls Metasys system 是美国江森自控（Johnson Controls）公司的一套楼宇自动化系统。

Johnson Controls Metasys system 9.0 之前版本中存在信任管理问题漏洞，该漏洞源于 Metasys ADS/ADX 服务器和 NAE/NIE/NCE 引擎使用共享的 RSA 密钥对来进行加密操作。攻击者可借助共享的 RSA 密钥对利用该漏洞解密 Metasys ADS/ADX 服务器或 NAE/NIE/NCE 引擎与之相连的 SMP 用户客户端之间捕获到的网络流量。

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.johnsoncontrols.com/

3. Palo Alto Networks PAN-OS 输入验证错误漏洞（CNNVD-201908-1857）

Palo Alto Networks PAN-OS 是美国 Palo Alto Networks 公司的一套为其防火墙设备开发的操作系统。

Palo Alto Networks PAN-OS 中存在输入验证错误漏洞。远程攻击者可通过发送恶意的消息利用该漏洞执行任意代码。以下产品及版本受到影响：

- Palo Alto Networks PAN-OS 7.1.24 及之前版本

- Palo Alto Networks PAN-OS 8.0.19 及之前版本
- Palo Alto Networks PAN-OS 8.1.9 及之前版本
- Palo Alto Networks PAN-OS 9.0.3 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://securityadvisories.paloaltonetworks.com/Home/Detail/160

4. **Cisco Small Business 220 Series Smart Switches 授权问题漏洞（CNNVD-201908-422）**

Cisco Small Business 220 Series Smart Switches 是美国思科（Cisco）公司的一款小型智能交换机设备。

使用 1.1.4.4 之前版本固件的 Cisco Small Business 220 Series Smart Switches 中的 Web 管理界面存在授权问题漏洞，该漏洞源于不完全的权限检查。远程攻击者可通过发送恶意的请求利用该漏洞上传任意文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass

5. **Adobe Creative Cloud Desktop Application 权限许可和访问控制问题漏洞(CNNVD-201908-722)**

Adobe Creative Cloud Desktop Application 是美国奥多比（Adobe）公司的一套用于在Creative云会员管理中心管理应用程序和服务的应用程序。该程序支持同步和共享文件、管理字体以及访问商业摄影和设计的资产库。

基于 Windows 和 macOS 平台的 Adobe Creative Cloud Desktop Application 4.6.1 及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/creative-cloud/apsb19-39.html

6. Adobe Photoshop 命令注入漏洞(CNNVD-201908-800)

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。

基于 Windows 和 macOS 平台的 Adobe Photoshop CC 19.1.8 及之前版本和 20.0.5 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/photoshop/apsb19-44.html"

7. NetApp Clustered Data ONTAP 加密问题漏洞(CNNVD-201908-353)

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 8.2.5P3 之前版本（7-Mode）中的 SMB 存在加密问题漏洞。攻击者可利用该漏洞泄露信息，添加或删除数据。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://security.netapp.com/advisory/ntap-20190802-0002/

8. Microsoft Windows DHCP 客户端缓冲区错误漏洞(CNNVD-201908-1005)

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。Windows DHCP Client 是其中的一个动态主机 IP 配置协议客户端。

Microsoft Windows DHCP 客户端中存在缓冲区错误漏洞。攻击者可通过发送特制的 DHCP 响应利用该漏洞在客户端设备上执行任意代码。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 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 版本 1803

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-2019-0736

9. eQ-3 HomeMatic CCU2 和 eQ-3 Homematic CCU3 访问控制错误漏洞(CNNVD-201908-1090)

eQ-3 Homematic CCU3 和 eQ-3 HomeMatic CCU2 都是德国 eQ-3 公司的一款智能家居系统的中央控制单元。

eQ-3 Homematic CCU2 2.47.10 之前版本和 eQ-3 Homematic CCU3 3.47.10 之前版本中的 JSON API 存在访问控制错误漏洞。攻击者可利用该漏洞读取、设置及删除元数据。

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.eq-3.com/

10. Android 代码问题漏洞(CNNVD-201908-399)

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 compiler.cc 文件中的 CompilationJob::FinalizeJob 存在代码问题漏洞。攻击者可利用该漏洞提升权限。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
- Android 9 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/2019-08-01.html

11. Cisco Enterprise NFV Infrastructure Software 操作系统命令注入漏洞(CNNVD-201908-558)

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 3.6.2 版本至 3.8.1 版本中的 Web 门户存在操作系统命令注入漏洞，该漏洞源于 Web 门户框架没有进行充分的输入验证。远程攻击者可借助恶意的输入利用该漏洞以 root 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://bst.cloudapps.cisco.com/bugsearch/bug/CSCvm76628

12. HPE 3PAR Service Processor 安全特征问题漏洞(CNNVD-201908-624)

HPE 3PAR Service Processor 是美国惠普企业公司（Hewlett Packard Enterprise，HPE）的一套 3PAR（存储产品）服务处理软件。

HPE 3PAR Service Processor 5.0.5.1 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安全限制。

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-hpesbst03942en_us

13. IBM Emptoris Contract Management SQL 注入漏洞（CNNVD-201908-1234）

IBM Emptoris Contract Management 是美国 IBM 公司的一套可实现合同生命周期自动化的软件。该软件可以自动执行和管理合同生命周期的各个阶段，如从合同及修正案的创建、执行和再协商，到绩效监控、分析和续订。

IBM Emptoris Contract Management 10.1.0 版本至 10.1.3 版本中存在 SQL 注入漏洞。远程攻击者可通过发送特制的 SQL 语句利用该漏洞查看、添加、更改或删除后端数据库中的信息。

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=ibm10880223

1.4.2 高危漏洞实例

本月高危漏洞共 576 个，其中重点漏洞实例如表 6 所示。

表 6　2019 年 8 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-201908-1078	eQ-3	eQ-3 Homematic CCU2 和 eQ-3 Homematic CCU3 资源管理错误漏洞（CNNVD-201908-1078）
		CNNVD-201908-151	Rockwell Automation	

		CNNVD-201908-2187	Red Hat	
		CNNVD-201908-1217	Linux	
		CNNVD-201908-1218		
		CNNVD-201908-1224		
		CNNVD-201908-1297		
		CNNVD-201908-1246	IBM	
		CNNVD-201908-2087	Google	
		CNNVD-201908-408		
		CNNVD-201908-411		
		CNNVD-201908-504		
		CNNVD-201908-2141	Cisco	
		CNNVD-201908-2152		
		CNNVD-201908-564		
		CNNVD-201908-1924	Autodesk	
		CNNVD-201908-738	Adobe	
		CNNVD-201908-756		
		CNNVD-201908-759		
		CNNVD-201908-763		
		CNNVD-201908-767		
		CNNVD-201908-779		
		CNNVD-201908-156	3S-Smart Software Solutions	
2	注入	CNNVD-201908-058	cPanel	cPanel 注入漏洞（CNNVD-201908-058）
		CNNVD-201908-477		
		CNNVD-201908-479		
		CNNVD-201908-530	Enhancesoft	
		CNNVD-201908-634	HPE	

3	信息泄露	CNNVD-201908-1042	ZOHO	Microsoft Windows RDP Server 信息泄露漏洞（CNNVD-201908-961）
		CNNVD-201908-1710	Cisco	
		CNNVD-201908-1995	kaseya	
		CNNVD-201908-271	Magento	
		CNNVD-201908-395	cPanel	
		CNNVD-201908-485		
		CNNVD-201908-487		
		CNNVD-201908-488		
		CNNVD-201908-725	Adobe	
		CNNVD-201908-833	floragunn	
		CNNVD-201908-961	Microsoft	
		CNNVD-201908-965		
4	信任管理问题	CNNVD-201908-2138	Knowage	Knowage 信任管理问题漏洞（CNNVD-201908-2138）
		CNNVD-201908-333	cPanel	
		CNNVD-201908-946	GitLab	
5	输入验证错误	CNNVD-201908-1836	普联	TP-Link TL-WR840N 输入验证错误漏洞（CNNVD-201908-1836）
		CNNVD-201908-1131	Yandex	
		CNNVD-201908-907	SAP	
		CNNVD-201908-929	Red Hat	
		CNNVD-201908-1193	Open-Xchange	
		CNNVD-201908-467	NVIDIA	
		CNNVD-201908-1003	Microsoft	
		CNNVD-201908-1013		
		CNNVD-201908-1021		
		CNNVD-201908-1022		
		CNNVD-201908-887		
		CNNVD-201908-889		

		CNNVD-201908-966		
		CNNVD-201908-980		
		CNNVD-201908-986		
		CNNVD-201908-990		
		CNNVD-201908-1074	McAfee	
		CNNVD-201908-829	Linux	
		CNNVD-201908-1086	IBM	
		CNNVD-201908-386	Google	
		CNNVD-201908-329	cPanel	
		CNNVD-201908-338		
		CNNVD-201908-391		
		CNNVD-201908-392		
		CNNVD-201908-394		
		CNNVD-201908-404		
		CNNVD-201908-476		
		CNNVD-201908-480		
		CNNVD-201908-481		
		CNNVD-201908-484		
		CNNVD-201908-486		
		CNNVD-201908-2132	CloudBees	
		CNNVD-201908-1694	Cisco	
		CNNVD-201908-1719		
		CNNVD-201908-2147		
		CNNVD-201908-2150		
		CNNVD-201908-2151		
		CNNVD-201908-413		
		CNNVD-201908-534		

		CNNVD-201908-537		
		CNNVD-201908-541		
		CNNVD-201908-545		
		CNNVD-201908-547		
		CNNVD-201908-788	Adobe	
		CNNVD-201908-791		
6	授权问题	CNNVD-201908-031	Apache	Intel Driver & Support Assistant 授权问题漏洞（CNNVD-201908-1257）
		CNNVD-201908-1253	Intel	
		CNNVD-201908-1256		
		CNNVD-201908-1257		
		CNNVD-201908-1258		
		CNNVD-201908-1636	Cisco	
		CNNVD-201908-1707		
		CNNVD-201908-1711		
		CNNVD-201908-546		
		CNNVD-201908-429	MongoDB	
		CNNVD-201908-450	NVIDIA	
		CNNVD-201908-633	HPE	
		CNNVD-201908-635		
		CNNVD-201908-882	SAP	
		CNNVD-201908-934	Red Hat	
7	权限许可和访问控制问题	CNNVD-201908-1733	Trend Micro	Netwrix Auditor 权限许可和访问控制问题漏洞（CNNVD-201908-708）
		CNNVD-201908-1922	Opera Software	
		CNNVD-201908-443	NVIDIA	
		CNNVD-201908-445		
		CNNVD-201908-708	Netwrix	

		CNNVD-201908-1000	Microsoft	
		CNNVD-201908-1008		
		CNNVD-201908-1009		
		CNNVD-201908-1014		
		CNNVD-201908-1016		
		CNNVD-201908-1017		
		CNNVD-201908-1025		
		CNNVD-201908-880		
		CNNVD-201908-892		
		CNNVD-201908-958		
		CNNVD-201908-959		
		CNNVD-201908-970		
		CNNVD-201908-973		
		CNNVD-201908-982		
		CNNVD-201908-983		
		CNNVD-201908-988		
		CNNVD-201908-989		
		CNNVD-201908-991		
		CNNVD-201908-996		
		CNNVD-201908-997		
		CNNVD-201908-998		
		CNNVD-201908-999		
		CNNVD-201908-292	Magento	
		CNNVD-201908-1226	IBM	
		CNNVD-201908-1229		
		CNNVD-201908-299		
		CNNVD-201908-393	Google	

		CNNVD-201908-396		
		CNNVD-201908-405		
		CNNVD-201908-415		
		CNNVD-201908-418		
		CNNVD-201908-427		
		CNNVD-201908-1895	floragunn	
		CNNVD-201908-909	ESTsoft	
		CNNVD-201908-649	Dell	
		CNNVD-201908-650		
		CNNVD-201908-1680	Cisco	
		CNNVD-201908-2156		
8	命令注入	CNNVD-201908-1080	普联	Adobe Photoshop 命令注入漏洞（CNNVD-201908-823）
		CNNVD-201908-1108	中兴	
		CNNVD-201908-1243	IBM	
		CNNVD-201908-1852	Docker	
		CNNVD-201908-823	Adobe	
		CNNVD-201908-911	eQ-3	
		CNNVD-201908-913		
9	路径遍历	CNNVD-201908-1251	IBM	IBM API Connect 路径遍历漏洞（CNNVD-201908-1251）
		CNNVD-201908-1729	ProSyst Softoware	
		CNNVD-201908-1731		
		CNNVD-201908-1917	Micro Focus	
		CNNVD-201908-275	Magento	
10	跨站请求伪造	CNNVD-201908-1069	OSIsoft	Cisco HyperFlex Software 跨站请求伪造漏洞（CNNVD-201908-565）
		CNNVD-201908-1126	Yandex	
		CNNVD-201908-1239	IBM	
		CNNVD-201908-1649	Cisco	

		CNNVD-201908-565		
		CNNVD-201908-1943	MicroPyramid	
		CNNVD-201908-279	Magento	
		CNNVD-201908-498	CloudBees	
11	跨站脚本	CNNVD-201908-056	cPanel	cPanel 跨站脚本漏洞（CNNVD-201908-056）
		CNNVD-201908-916	TIBCO Software	
12	竞争条件问题	CNNVD-201908-420	Google	Android Framework 组件竞争条件问题漏洞（CNNVD-201908-420）
13	加密问题	CNNVD-201908-1634	Cisco	Cisco HyperFlex Software 加密问题漏洞（CNNVD-201908-1634）
		CNNVD-201908-274	Magento	
		CNNVD-201908-276		
		CNNVD-201908-290		
		CNNVD-201908-526	Apache	
14	缓冲区错误	CNNVD-201908-167	研华	Advantech WebAccess HMI Designer 缓冲区错误漏洞（CNNVD-201908-167）
		CNNVD-201908-308	Vmware	
		CNNVD-201908-872	SAP	
		CNNVD-201908-1861	Palo Alto Networks	
		CNNVD-201908-1006	Microsoft	
		CNNVD-201908-1023		
		CNNVD-201908-857		
		CNNVD-201908-860		
		CNNVD-201908-902		
		CNNVD-201908-908		
		CNNVD-201908-915		
		CNNVD-201908-926		
		CNNVD-201908-954		

		CNNVD-201908-956		
		CNNVD-201908-957		
		CNNVD-201908-969		
		CNNVD-201908-971		
		CNNVD-201908-974		
		CNNVD-201908-975		
		CNNVD-201908-976		
		CNNVD-201908-979		
		CNNVD-201908-984		
		CNNVD-201908-987		
		CNNVD-201908-992		
		CNNVD-201908-993		
		CNNVD-201908-994		
		CNNVD-201908-1161	Linux	
		CNNVD-201908-1219		
		CNNVD-201908-1222		
		CNNVD-201908-1223		
		CNNVD-201908-2032		
		CNNVD-201908-2176		
		CNNVD-201908-2180		
		CNNVD-201908-2185		
		CNNVD-201908-389	Google	
		CNNVD-201908-1135	Fuji Electric	
		CNNVD-201908-2261	ESTsoft	
		CNNVD-201908-906		
		CNNVD-201908-939	Delta Electronics	

		CNNVD-201908-905	Korea Electronic Certification Authority	
		CNNVD-201908-1678	Cisco	
		CNNVD-201908-535		
		CNNVD-201908-538		
		CNNVD-201908-539		
		CNNVD-201908-540		
		CNNVD-201908-542		
		CNNVD-201908-544		
		CNNVD-201908-1029	Artifex Software	
		CNNVD-201908-1098	Apache	
		CNNVD-201908-262		
		CNNVD-201908-277		
		CNNVD-201908-727	Adobe	
		CNNVD-201908-728		
		CNNVD-201908-730		
		CNNVD-201908-731		
		CNNVD-201908-733		
		CNNVD-201908-734		
		CNNVD-201908-735		
		CNNVD-201908-736		
		CNNVD-201908-739		
		CNNVD-201908-742		
		CNNVD-201908-745		
		CNNVD-201908-747		

		CNNVD-201908-766		
		CNNVD-201908-769		
		CNNVD-201908-784		
		CNNVD-201908-785		
		CNNVD-201908-793		
		CNNVD-201908-794		
		CNNVD-201908-795		
		CNNVD-201908-796		
		CNNVD-201908-797		
		CNNVD-201908-798		
		CNNVD-201908-808		
		CNNVD-201908-810		
		CNNVD-201908-811		
		CNNVD-201908-812		
		CNNVD-201908-814		
		CNNVD-201908-815		
		CNNVD-201908-816		
		CNNVD-201908-819		
		CNNVD-201908-820		
		CNNVD-201908-822		
		CNNVD-201908-824		
		CNNVD-201908-830		
		CNNVD-201908-837		
		CNNVD-201908-844		
15	访问控制错误	CNNVD-201908-1081	eQ-3	Tenable Network Security Nessus 访问控制问题漏洞（CNNVD-201908-1096）
		CNNVD-201908-1096	Tenable Network Security	

		CNNVD-201908-1259	Intel	
		CNNVD-201908-1260		
		CNNVD-201908-1650	Cisco	
		CNNVD-201908-2177	奇偶科技	
		CNNVD-201908-312	Avira Operations	
		CNNVD-201908-403	cPanel	
		CNNVD-201908-478		
		CNNVD-201908-444	NVIDIA	
16	代码注入	CNNVD-201908-901	SAP	SAP Commerce Cloud 代码注入漏洞（CNNVD-201908-901）
17	代码问题	CNNVD-201908-1002	Microsoft	Microsoft Windows 和 Windows Server 代码问题漏洞（CNNVD-201908-903）
		CNNVD-201908-580	ZOHO	
		CNNVD-201908-582		
		CNNVD-201908-1300	Trend Micro	
		CNNVD-201908-1301		
		CNNVD-201908-1735		
		CNNVD-201908-1250	Rapid7	
		CNNVD-201908-1738		
		CNNVD-201908-449	Qualcomm	
		CNNVD-201908-903	Microsoft	
		CNNVD-201908-294	Magento	
		CNNVD-201908-141	LCDS	
		CNNVD-201908-1099	IBM	
		CNNVD-201908-1249		
		CNNVD-201908-1858		
		CNNVD-201908-364		
		CNNVD-201908-611		

		CNNVD-201908-622	HPE	
		CNNVD-201908-2223	Citrix Systems	
		CNNVD-201908-1705	Cisco	
		CNNVD-201908-1648	Bitdefender	
		CNNVD-201908-1923	Autodesk	
		CNNVD-201908-718	Adobe	
		CNNVD-201908-723		
		CNNVD-201908-724		
		CNNVD-201908-743		
		CNNVD-201908-817		
18	安全特征问题	CNNVD-201908-1244	IBM	IBM Security Guardium Big Data Intelligence 安全特征问题漏洞（CNNVD-201908-1244）
		CNNVD-201908-313	cPanel	
		CNNVD-201908-340		
		CNNVD-201908-374	Qualcomm	
		CNNVD-201908-620	Jitbit Software	
		CNNVD-201908-721	Adobe	
19	SQL 注入	CNNVD-201908-1949	Cybozu	Cybozu Garoon SQL 注入漏洞（CNNVD-201908-1949）
		CNNVD-201908-705	Frappe Technologies	

1. eQ-3 Homematic CCU2 和 eQ-3 Homematic CCU3 资源管理错误漏洞（CNNVD-201908-1078）

eQ-3 Homematic CCU3 和 eQ-3 HomeMatic CCU2 都是德国 eQ-3 公司的一款智能家居系统的中央控制单元。

eQ-3 Homematic CCU2 和 eQ-3 Homematic CCU3 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。以下产品及版本受到影响：

- eQ-3 Homematic CCU2 2.35.16 版本
- eQ-3 Homematic CCU2 2.41.5 版本
- eQ-3 Homematic CCU2 2.41.8 版本
- eQ-3 Homematic CCU2 2.41.9 版本
- eQ-3 Homematic CCU2 2.45.6 版本
- eQ-3 Homematic CCU2 2.45.7 版本
- eQ-3 Homematic CCU2 2.47.10 版本
- eQ-3 Homematic CCU2 2.47.12 版本
- eQ-3 Homematic CCU2 2.47.15 版本
- eQ-3 Homematic CCU3 3.41.11 版本
- eQ-3 Homematic CCU3 3.43.16 版本
- eQ-3 Homematic CCU3 3.45.5 版本
- eQ-3 Homematic CCU3 3.45.7 版本
- eQ-3 Homematic CCU3 3.47.10 版本
- eQ-3 Homematic CCU3 3.47.15 版本

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://www.eq-3.com/

2. cPanel 注入漏洞（CNNVD-201908-058）

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 70.0.23 之前版本中存在注入漏洞。攻击者可利用该漏洞向 cPanel 会话文件中注入任意的数据。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://documentation.cpanel.net/display/CL/70+Change+Log

3. Microsoft Windows RDP Server 信息泄露漏洞（CNNVD-201908-961）

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。RDP Server 其中的一个远程桌面协议（RDP）服务器。

Microsoft Windows RDP Server 中存在信息泄露漏洞。攻击者可借助特制的应用程序利用该漏洞获取信息。以下产品及版本受到影响：

- Microsoft Windows 10 版本 1803
- Microsoft Windows 10 版本 1809
- Microsoft Windows 10 版本 1903
- 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-2019-1225

4. Knowage 信任管理问题漏洞（CNNVD-201908-2138）

Knowage 是意大利 Knowage 公司的一套用于在传统资源和大数据系统上进行现代业务分析的开源套件。

Knowage 中存在信任管理问题漏洞。攻击者可利用该漏洞获取明文形式的数据源凭证（包括：数据库）。

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.knowage-suite.com

5. TP-Link TL-WR840N 输入验证错误漏洞（CNNVD-201908-1836）

TP-Link TL-WR840N 是中国普联（TP-Link）的一款无线路由器。

使用 0.9.1 3.16 及之前版本固件的 TP-Link TL-WR840N v4 版本中的‘traceroute’函数存在输入验证错误漏洞。攻击者可借助 IP 地址输入字段中特制的 payload 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.tp-link.com/

6. Intel Driver & Support Assistant 授权问题漏洞（CNNVD-201908-1257）

Intel Driver & Support Assistant 是美国英特尔（Intel）公司的一款 Intel 驱动程序和支持管理工具。该工具主要用于获取 Intel 提供的最新应用程序。

Intel Driver & Support Assistant 19.7.30.2 之前版本中存在授权问题漏洞，该漏洞源于程序没有正确验证文件。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-00276.html

7. Netwrix Auditor 权限许可和访问控制问题漏洞（CNNVD-201908-708）

Netwrix Auditor 是美国 Netwrix 公司的一套 IT 审计软件。该软件具有用户行为分析、安全威胁主动检测和威胁类型警报等功能。

Netwrix Auditor 9.8 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以 NT AUTHORITYSYSTEM 权限执行代码。

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.netwrix.com/

8. Adobe Photoshop 命令注入漏洞（CNNVD-201908-823）

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。

基于 Windows 和 macOS 平台的 Adobe Photoshop CC 19.1.8 及之前版本和 20.0.5 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/photoshop/apsb19-44.html

9. IBM API Connect 路径遍历漏洞（CNNVD-201908-1251）

IBM API Connect（APIConnect）是美国 IBM 公司的一套用于管理 API 生命周期的集成解决方案。该产品支持创建、运行、管理和保护 API 和微服务等。

IBM API Connect 5.0.0.0 版本至 5.0.8.6 版本中存在路径遍历漏洞。攻击者可通过发送特制的 URL 请求利用该漏洞查看系统上的任意文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www-01.ibm.com/support/docview.wss?uid=ibm10960848

10. Cisco HyperFlex Software 跨站请求伪造漏洞（CNNVD-201908-565）

Cisco HyperFlex Software 是美国思科（Cisco）公司的一套套可扩展的分布式文件系统。该系统通过云管理提供统一的计算、存储和网络，并提供企业级数据管理和优化服务。

Cisco HyperFlex Software 4.0(2a)及之前版本中的 Web 管理界面存在跨站请求伪造漏洞。远程攻击者可通过诱使用户访问恶意的链接利用该漏洞执行恶意的操作。

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-20190807-hypflex-csrf

11. cPanel 跨站脚本漏洞（CNNVD-201908-056）

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 70.0.23 之前版本中存在跨站脚本漏洞。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://documentation.cpanel.net/display/CL/70+Change+Log

12. Android Framework 组件竞争条件问题漏洞（CNNVD-201908-420）

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。Framework 是其中的一个 Android 框架组件。

Android 9 版本中的 Framework 存在竞争条件问题漏洞。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://source.android.com/security/bulletin/2019-08-01.html

13. Cisco HyperFlex Software 加密问题漏洞（CNNVD-201908-1634）

Cisco HyperFlex Software 是美国思科（Cisco）公司的一套套可扩展的分布式文件系统。该系统通过云管理提供统一的计算、存储和网络，并提供企业级数据管理和优化服务。

Cisco HyperFlex Software 4.0(1a)之前版本中存在加密问题漏洞，该漏洞源于程序没有充分进行密钥管理。远程攻击者可通过获取密钥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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory

/cisco-sa-20190821-hyperflex-sslkey

14. Advantech WebAccess HMI Designer 缓冲区错误漏洞（CNNVD-201908-167）

Advantech WebAccess HMI Designer 是中国台湾研华（Advantech）公司的一款人机界面集成开发工具。该产品具备数据传输、菜单编辑和文本编辑等功能。

Advantech WebAccess HMI Designer 2.1.9.23 及之前版本中存在缓冲区错误漏洞，该漏洞源于程序没有正确地验证用户提交的数据。攻击者可借助 MCR 文件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.advantech.com/

15. Tenable Network Security Nessus 访问控制错误漏洞（CNNVD-201908-1096）

Tenable Network Security Nessus 是美国 Tenable Network Security 公司的一款开源的系统漏洞扫描器。

基于 Windows 平台的 Tenable Network Security Nessus 8.5.2 及之前版本中存在访问控制错误漏洞。攻击者可利用该漏洞覆盖任意系统文件，可能造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.tenable.com/security/tns-2019-05

16. SAP Commerce Cloud 代码注入漏洞（CNNVD-201908-901）

SAP Commerce Cloud 是德国思爱普（SAP）公司的一套基于云的

电子商务平台。该产支持销售管理、营销管理、订单管理和运营管理等。

SAP Commerce Cloud 中存在代码注入漏洞。攻击者可利用该漏洞控制该应用程序的运行。以下产品及版本受到影响：

- SAP Commerce Cloud 6.4 版本
- SAP Commerce Cloud 6.5 版本
- SAP Commerce Cloud 6.6 版本
- SAP Commerce Cloud 6.7 版本
- SAP Commerce Cloud 1808 版本
- SAP Commerce Cloud 1811 版本
- SAP Commerce Cloud 1905 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=523998017

17. Microsoft Windows 和 Windows Server 代码问题漏洞（CNNVD-201908-903）

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 和 Microsoft Windows Server 中存在代码问题漏洞，该漏洞源于 XmlLite runtime 没有正确解析 XML 输入。攻击者可通过发送特制的请求利用该漏洞造成拒绝服务。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-2019-1187

18. IBM Security Guardium Big Data Intelligence 安全特征问题漏洞（CNNVD-201908-1244）

IBM Security Guardium Big Data Intelligence（SonarG）是美国 IBM 公司的一套大数据安全智能解决方案。该方案具有交互式数据探索、自动连接分析和用户活动分析等特点。

IBM Security Guardium Big Data Intelligence 4.0 版本中存在安全特征问题漏洞，该漏洞源于程序没有限制过多的身份验证请求。远程攻击者可利用该漏洞暴力破解账户凭证。

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=ibm10960298

19. Cybozu Garoon SQL 注入漏洞（CNNVD-201908-1949）

Cybozu Garoon 是日本才望子（Cybozu）公司的一套门户型 OA 办公系统。该系统提供门户、E-mail、书签、日程安排、公告栏、文件管理等功能。

Cybozu Garoon 4.0.0 版本至 4.10.3 版本中存在 SQL 注入漏洞。远程攻击者可利用该漏洞获取或修改存储在数据库中的信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://cs.cybozu.co.jp/2019/006951.html

二、接报漏洞情况

本月接报漏洞共计 5111 个，其中信息技术产品漏洞（通用型漏

洞）131 个，网络信息系统漏洞（事件型漏洞）4980 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	2650	0	2650
2	网神信息技术（北京）股份有限公司	1699	2	1697
3	内蒙古奥创科技有限公司	180	18	162
4	中新网络信息安全股份有限公司	135	0	135
5	西安四叶草信息技术有限公司	114	26	88
6	北京数字观星科技有限公司	79	0	79
7	山东新潮信息技术有限公司	78	0	78
8	北京天融信网络安全技术有限公司	42	42	0
9	北京圣溥润高新技术服份有限公司	30	0	30
10	广州锦行网络科技有限公司	21	1	20
11	上海安识网络科技有限公司	15	0	15
12	北京神州绿盟科技有限公司安全研究部	10	10	0
13	国发中新（北京）科技发展有限公司	10	0	10
14	福建经联网络技术有限公司	8	0	8
15	天津市兴先道科技有限公司	8	8	0
16	个人	7	4	3
17	广州万方计算机科技有限公司	4	4	0
18	西安交大捷普网络科技有限公司	4	3	1
19	东软集团股份有限公司	2	2	0

20	北京威努特技术有限公司	2	2	0
21	厦门服云信息科技有限公司	2	2	0
22	中兴通讯	2	1	1
23	中科汇能科技有限公司	2	0	2
24	国网浙江省电力有限公司温州供电公司、北京神州绿盟科技有限公司	1	1	0
25	国网浙江省电力有限公司电力科学研究院、国网浙江省电力有限公司温州供电公司	1	1	0
26	北京中金安服科技有限公司	1	0	1
27	四川虹微技术有限公司	1	1	0
28	北京安信天行科技有限公司	1	1	0
29	中国电信集团系统集成有限责任公司云计算安全与服务事业部	1	1	0
30	梆梆安全	1	1	0
报送总计		5111	131	4980

三、重大漏洞预警

3.1 关于 Apache Solr 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 Apache Solr 远程代码执行漏洞（CNNVD-201908-031、CVE-2019-0193）情况的报送。成功利用漏洞的攻击者，可在目标服务器上远程执行恶意代码。Apache Solr 8.2.0 之前版本均受漏洞影响。目前，Apache 官方已发布升级补丁修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

Apache Solr 是美国阿帕奇（Apache）软件基金会的一款基于 Lucene（一款全文搜索引擎）的搜索服务器，它对外提供类似于 Web-service 的 API 接口，被很多企业广泛使用。漏洞源于 Apache Solr DataImportHandler 模块的 DIH 管理界面在开启调试模式时，DIH 配置可以接收来自请求的 dataConfig 参数，通过该参数可以包含恶意脚本导致代码执行。

漏洞危害

目前，漏洞细节和利用代码暂未公开，但攻击者可以通过补丁对比方式分析出漏洞触发点，并进一步开发漏洞利用代码。成功利用漏洞的攻击者，可在目标服务器上远程执行恶意代码。Apache Solr 8.2.0 之前版本均受漏洞影响

修复措施

目前，Apache 官方已发布升级补丁修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方补丁链接如下：

http://lucene.apache.org/solr/downloads.html。

3.2 关于 Fortinet FortiOS 多个安全漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Fortinet FortiOS 多个安全漏洞情况的报送。包括 Fortinet FortiOS 路径遍历漏洞（CNNVD-201905-1026、CVE-2018-13379）、Fortinet FortiOS 跨站脚本漏洞（CNNVD-201905-1024、CVE-2018-13380）等多个漏洞。成功利用漏洞的攻击者，可在未经身份验证的情况下获取用户账号敏感信息，修改账号密码，从而最终控制目标系统。Fortinet FortiOS 5.6.3 版本至 5.6.7 版本、6.0.0 版本至 6.0.4 版本等多个版本均受此漏洞影响。目前，Fortigate 官方已发布升级补丁修复了该漏洞，建议用户尽快将 Fontigate 升级到 FortiOS 5.4.11、5.6.9、6.0.5、6.2.0 或更高版本，从而修补漏洞带来的危害。

漏洞简介

Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、VPN、Web 内容过滤和反垃圾邮件等多种安全功能。在 2019 年 blackhat 上，安全研究人员公布了 Fortinet FortiOS 多个漏洞，包括

Fortinet FortiOS 路径遍历漏洞（CNNVD-201905-1026、CVE-2018-13379）、Fortinet FortiOS 跨站脚本漏洞（CNNVD-201905-1024、CVE-2018-13380）、Fortinet FortiOS 缓冲区错误漏洞（CNNVD-201905-878、CVE-2018-13381）（CNNVD-201904-116、CVE-2018-13383）、Fortinet FortiOS 授权问题漏洞（CNNVD-201905-1025、CVE-2018-13382）等。成功利用漏洞的攻击者，可在未经身份验证的情况下获取用户账号敏感信息，修改账号密码，从而最终控制目标系统。漏洞详情如下：

1、Fortinet FortiOS 路径遍历漏洞（CNNVD-201905-1026、CVE-2018-13379）

漏洞源于该系统未能正确地过滤资源或文件路径中的特殊元素，导致攻击者可以利用该漏洞访问受限目录以外的位置。Fortinet FortiOS 5.6.3 版本至 5.6.7 版本、6.0.0 版本至 6.0.4 版本中的 SSL VPN 受此漏洞影响。

2、Fortinet FortiOS 跨站脚本漏洞（CNNVD-201905-1024、CVE-2018-13380）

漏洞源于 WEB 应用缺少对客户端数据的正确验证，导致攻击者可利用该漏洞执行客户端代码。Fortinet FortiOS 6.0.0 版本至 6.0.4 版本、5.6.0 版本至 5.6.7 版本、5.4 及之前版本中的 SSL VPN 受此漏洞影响。

3、Fortinet FortiOS 缓冲区错误漏洞（CNNVD-201905-878、CVE-2018-13381）（CNNVD-201904-116、CVE-2018-13383）

漏洞源于该系统在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作，攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。Fortinet FortiOS 6.2.0 之前版本受此漏洞影响。

4、Fortinet FortiOS 授权问题漏洞（CNNVD-201905-1025、CVE-2018-13382）

漏洞源于该系统中缺少身份验证措施或身份验证强度不足，导致攻击者可以修改任意用户的密码。Fortinet FortiOS 6.0.0 版本至 6.0.4 版本、5.6.0 版本至 5.6.8 版本、5.4.1 版本至 5.4.10 版本受此漏洞影响。

漏洞危害

目前，漏洞利用代码已公开，Fortinet FortiOS 多个版本均受漏洞影响，具体影响版本如下：

	漏洞名称	影响版本
1	Fortinet FortiOS 路径遍历漏洞（CNNVD-201905-1026、CVE-2018-13379）	Fortinet FortiOS 5.6.3 版本至 5.6.7 版本、6.0.0 版本至 6.0.4 版本
2	Fortinet FortiOS 跨站脚本漏洞（CNNVD-201905-1024、CVE-2018-13380）	Fortinet FortiOS 6.0.0 版本至 6.0.4 版本、5.6.0 版本至 5.6.7 版本、5.4 及之前版本

3	Fortinet FortiOS 缓冲区错误漏洞（CNNVD-201905-878、CVE-2018-13381）（CNNVD-201904-116、CVE-2018-13383）	Fortinet FortiOS 6.2.0 之前版本
4	Fortinet FortiOS 授权问题漏洞（CNNVD-201905-1025、CVE-2018-13382）	Fortinet FortiOS 6.0.0 版本至 6.0.4 版本、5.6.0 版本至 5.6.8 版本、5.4.1 版本至 5.4.10 版本

安全建议

目前，Fortigate 官方已发布升级补丁修复了该漏洞，建议用户尽快将 Fontigate 升级到 FortiOS 5.4.11、5.6.9、6.0.5、6.2.0 或更高版本，从而修补漏洞带来的危害。官方补丁链接如下：

	漏洞名称	漏洞补丁地址
1	Fortinet FortiOS 路径遍历漏洞（CNNVD-201905-1026、CVE-2018-13379）	https://fortiguard.com/psirt/FG-IR-18-384
2	Fortinet FortiOS 跨站脚本漏洞（CNNVD-201905-102	https://fortiguard.com/psirt/FG-IR-18-383

	4、CVE-2018-13380）	
3	Fortinet FortiOS 缓冲区错误漏洞（CNNVD-201905-878、CVE-2018-13381）（CNNVD-201904-116、CVE-2018-13383）	https://fortiguard.com/psirt/FG-IR-18-387 https://fortiguard.com/psirt/FG-IR-18-389
4	Fortinet FortiOS 授权问题漏洞（CNNVD-201905-1025、CVE-2018-13382）	https://fortiguard.com/psirt/FG-IR-18-388

。