北京师范大学网络信息安全通告

2019 年 10月报告

北京师范大学信息网络中心

2019 年 11 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 10 月份新增安全漏洞共 1774 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 137 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 15.11%。本月新增漏洞中，超危漏洞 202 个、高危漏洞 581 个、中危漏洞 916 个、低危漏洞 75 个，相应修复率分别为 76.73%、82.27%、83.62%以及 85.33%。合计 1463 个漏洞已有修复补丁发布，本月整体修复率 82.47%。

截至 2019 年 10 月 31 日，CNNVD 采集漏洞总量已达 134943 个。

1.1 漏洞增长概况

2019 年 10 月新增安全漏洞 1774 个，与上月（1377 个）相比增多了 28.83%。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 1612 个。

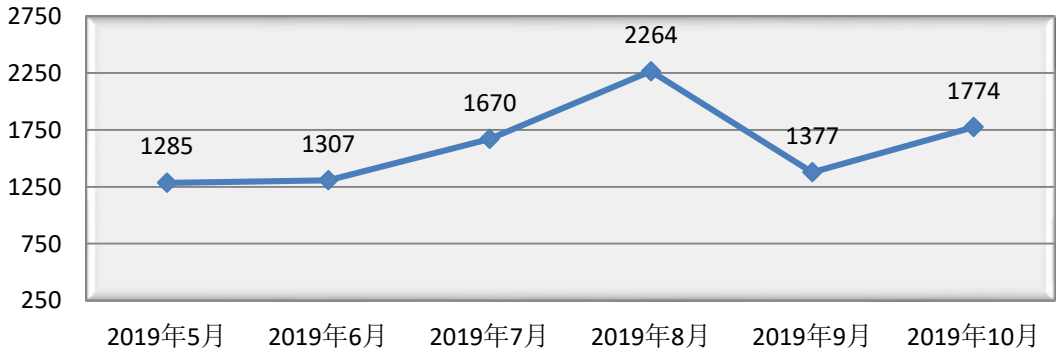

图 1 2019 年 5 月至 2019 年 10 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

10 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司达到 137 个，占本月漏洞总量的 7.72%。本月 Oracle、思科、Adobe 等公司的漏洞数量均有所上升，微软、谷歌等厂商的漏洞数量出现较不同程度的下降。

表 1　2019 年 10 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	137	7.72%
2	思科	85	4.79%
3	Adobe	84	4.74%
4	苹果	73	4.11%
5	微软	59	3.33%
6	Magento	58	3.27%
7	IBM	46	2.59%
8	CloudBees	46	2.59%
9	谷歌	41	2.31%
10	JetBrains	34	1.92%

1.2.2 漏洞产品分布

10 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 37 条，其中桌面操作系统 37 条，服务器操作系统 35 条。本月 Apple macOS 漏洞数量最多，共 42 个，占主流操作系统漏洞总量的 13.59%，排名第一。

表 2　2019 年 10 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Apple macOS	42

2	Apple iOS	34
3	Windows 10	33
4	Windows Server 1903	30
5	Windows Server 1803	29
6	Windows Server 2016	28
7	Windows 8.1	19
8	Windows Rt 8.1	19
9	Windows Server 2012	19
10	Windows Server 2008	19
11	Windows 7	18
12	Linux Kernel	10
13	Android	9

*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

10 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 15.11%。

表 32019 年 10 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	268	15.11%
2	缓冲区错误	188	10.60%
3	输入验证错误	146	8.23%
4	信息泄露	93	5.24%
5	SQL 注入	82	4.62%
6	代码问题	80	4.51%

7	资源管理错误	67	3.78%
8	路径遍历	48	2.71%
9	授权问题	42	2.37%
10	跨站请求伪造	36	2.03%
11	操作系统命令注入	28	1.58%
12	信任管理问题	21	1.18%
13	注入	17	0.96%
14	日志信息泄露	14	0.79%
15	访问控制错误	13	0.73%
16	代码注入	13	0.73%
17	权限许可和访问控制问题	7	0.39%
18	加密问题	7	0.39%
19	竞争条件问题	6	0.34%
20	命令注入	4	0.23%
21	后置链接	3	0.17%
22	数据伪造问题	2	0.11%
23	环境问题	1	0.06%
24	安全特征问题	1	0.06%
25	数字错误	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。10 月漏洞危害等级分布如图 2 所示，其中超危漏洞 202 条，占本月漏洞总数的 11.39%。

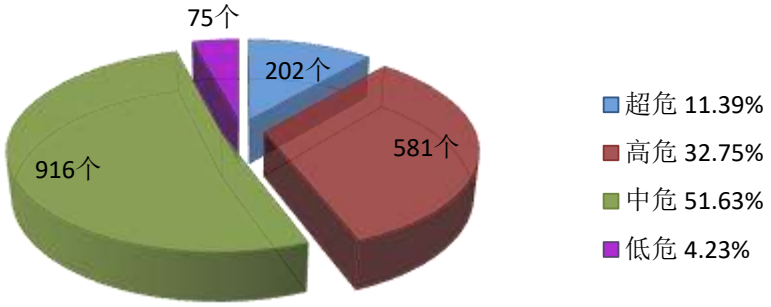

图 2　2019 年 10 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

10 月漏洞修复情况按危害等级进行统计见图 3。其中低漏洞修复率最高，达到 85.33%，超危漏洞修复率最低，比例为 76.73%。与上月相比，本月中危漏洞修复率有所上升，超、高、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 79.67%上升至本月的 82.47%。

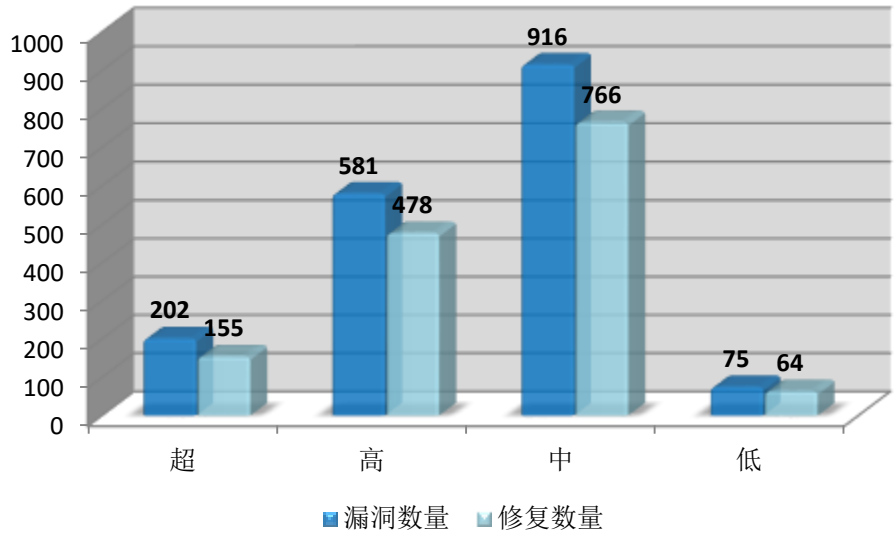

图 3　2019 年 10 月漏洞修复数量统计

1.3.2 厂商修复情况

10 月漏洞修复情况按漏洞数量前十厂商进行统计，其中谷歌、微软、GitLab 等十个厂商共 663 条漏洞，占本月漏洞总数的 37.37%，漏洞修复率为 94.87%，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、思科、Adobe、苹果、微软、Magento、Jetbrains 等公司本月漏洞修复率均为 100%，共 612 条漏洞已全部修复。

表 4　2019 年 10 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	137	137	100.00%
2	思科	85	85	100.00%
3	Adobe	84	84	100.00%
4	苹果	73	73	100.00%
5	微软	59	59	100.00%
6	Magento	58	58	100.00%
7	IBM	46	42	91.30%
8	CloudBees	46	18	39.13%
9	谷歌	41	39	95.12%
10	Jetbrains	34	34	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 202 个，其中重要漏洞实例如表 5 所示。

表 5　2019 年 10 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-201910-175	Facebook	Adobe Acrobat 和 Reader 资源管理错误漏洞（CNNVD-201910-833）
		CNNVD-201910-833	Adobe	
		CNNVD-201910-837		
		CNNVD-201910-900		
		CNNVD-201910-903		
		CNNVD-201910-904		
		CNNVD-201910-905		
		CNNVD-201910-907		
2	注入	CNNVD-201910-147	Jetbrains	Sophos Cyberoam firewall appliance CyberoamOS 注入漏洞（CNNVD-201910-727）
		CNNVD-201910-727	Sophos	
		CNNVD-201910-838	Adobe	
3	信任管理问题	CNNVD-201910-008	Broadcom	Broadcom CA Network Flow Analysis 信任管理问题漏洞（CNNVD-201910-008）
4	输入验证错误	CNNVD-201910-035	Jetbrains	Xiaomi Mi WiFi R3G 输入验证错误漏洞（CNNVD-201910-1434）
		CNNVD-201910-150		
		CNNVD-201910-1190	中华电信	
		CNNVD-201910-1212		
		CNNVD-201910-1434	小米科技	
		CNNVD-201910-1470	MapR	
		CNNVD-201910-1162	HP	
		CNNVD-201910-244	Activesoft	
5	授权问题	CNNVD-201910-1274	Citrix Systems	Cobham plc EXPLORER 710 授权问题漏洞（CNNVD-201910-704）
		CNNVD-201910-704	Cobham plc	
6	日志信息泄露	CNNVD-201910-926	Expedia	Dark Horse Comics application for Android 日志信息泄露漏洞（CNNVD-201910-933）
		CNNVD-201910-931	PowerSchool	
		CNNVD-201910-933	Dark Horse	
7	跨站脚本	CNNVD-201910-663	NetSarang	NetSarang XFTP Client 跨站脚本漏洞（CNNVD-201910-663）
8	加密问题	CNNVD-201910-1447	Adobe	Adobe Acrobat 和 Reader 加密问题漏洞（CNNVD-201910-1447）
9	缓冲区错误	CNNVD-201910-1387	Facebook	Microsoft Azure App Service on Azure Stack 缓冲区错误漏洞
		CNNVD-201910-145		
		CNNVD-201910-473	Microsoft	

		CNNVD-201910-485		（CNNVD-201910-473）
		CNNVD-201910-842	Adobe	
		CNNVD-201910-857		
		CNNVD-201910-861		
		CNNVD-201910-879		
10	访问控制错误	CNNVD-201910-1136	Cisco	Cisco Aironet Access Points Software 访问控制错误漏洞（CNNVD-201910-1136））
11	代码注入	CNNVD-201910-004	CloudBees	qibosoft 代码注入漏洞（CNNVD-201910-947）
		CNNVD-201910-947	齐博软件	
12	代码问题	CNNVD-201910-1171	NETGEAR	Cisco Security Manager 代码问题漏洞（CNNVD-201910-143）
		CNNVD-201910-143	Cisco	
		CNNVD-201910-843	Adobe	
		CNNVD-201910-848		
		CNNVD-201910-849		
		CNNVD-201910-852		
		CNNVD-201910-854		
		CNNVD-201910-855		
		CNNVD-201910-856		
13	操作系统命令注入	CNNVD-201910-243	Activesoft	Activesoft MyBuilder 操作系统命令注入漏洞（CNNVD-201910-243）
14	SQL 注入	CNNVD-201910-1493	Zend	ZOHO ManageEngine OpManager SQL 注入漏洞（CNNVD-201910-937）
		CNNVD-201910-152	Umbraco	
		CNNVD-201910-504	Magento	
		CNNVD-201910-531		
		CNNVD-201910-937	ZOHO	

1. Adobe Acrobat 和 Reader 资源管理错误漏洞（CNNVD-201910-833）

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 Reader 中存在资源管理错误漏洞。攻击者可利用该漏洞执行代码。基于 Windows 和 macOS 平台的以下产品及版本受

到影响：

- Adobe Acrobat DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat 2015（Classic 2015）2015.006.30503 及之前版本
- Adobe Acrobat Reader DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat Reader 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat Reader 2015（Classic 2015）2015.006.30503 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/apsb19-49.html

2. Sophos Cyberoam firewall appliance CyberoamOS 注入漏洞（CNNVD-201910-727）

Sophos Cyberoam firewall appliance 是英国 Sophos 公司的一款防火墙设备。CyberoamOS 是运行在其中的一套操作系统。

Sophos Cyberoam firewall appliance 中的 CyberoamOS 10.6.6 MR-6 之前版本存在注入漏洞。攻击者可借助 Web Admin 和 SSL VPN 控制台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://community.sophos.com/kb/en-us/134732

3. Broadcom CA Network Flow Analysis 信任管理问题漏洞（CNNVD-201910-008）

Broadcom CA Network Flow Analysis 是美国博通（Broadcom）公司的一套网络流量监视解决方案。

Broadcom CA Network Flow Analysis 9.x 版本和 10.0.x 版本中存在信任管理问题漏洞，该漏洞源于网络系统或产品中缺乏有效的信任管理机制。攻击者可利用默认密码或者硬编码密码、硬编码证书等攻击受影响组件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/new-security-notice-ca-20190930-01-security-notice-for-ca-network-flow-analysis.html

4. Xiaomi Mi WiFi R3G 输入验证错误漏洞（CNNVD-201910-1434）

Xiaomi Mi WiFi R3G 是中国小米科技（Xiaomi）公司的一款 3G 路由器。

Xiaomi Mi WiFi R3G 2.28.23-stable 之前版本中存在输入验证错误漏洞，该漏洞源于网络系统或产品未对输入的数据进行正确的验证。

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://www.mi.com

5. Cobham plc EXPLORER 710 授权问题漏洞（CNNVD-201910-704）

Cobham plc EXPLORER 710 是英国 Cobham plc 公司的一款便携式卫星终端设备。该产品主要提供卫星通信和互联网访问等功能。

使用 1.07 版本固件的 Cobham plc EXPLORER 710 中存在授权问题漏洞，该漏洞源于程序允许用户未经身份验证便可访问 5454 端口。远程攻击者可利用该漏洞连接到该端口并执行 AT 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.cobham.com

6. Dark Horse Comics application for Android 日志信息泄露漏洞（CNNVD-201910-933）

Dark Horse Comics application for Android 是美国黑马漫画（Dark Horse）公司的一款基于 Android 平台的在线漫画阅读应用程序。

基于 Android 平台的 Dark Horse Comics 应用程序 1.3.21 版本中存在日志信息泄露漏洞。该漏洞源于网络系统或产品的日志文件非正常输出。

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.darkhorse.com/

7. NetSarang XFTP Client 跨站脚本漏洞（CNNVD-201910-663）

NetSarang XFTP Client 是美国 NetSarang 公司的一款 FTP（文件传输协议）客户端应用程序。

NetSarang XFTP Client 6.0149 及之前版本中存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

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.netsarang.com

8. Adobe Acrobat 和 Reader 加密问题漏洞（CNNVD-201910-1447）

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 Reader 中存在加密问题漏洞。攻击者可利用该漏洞绕过安全功能。以下产品及版本受到影响：

- 基于 macOS 平台的 Adobe Acrobat DC （Continuous） 2019.012.20034 及之前版本
- 基于 macOS 平台的 Adobe Acrobat DC（Classic 2017） 2017.011.30142 及之前版本
- 基于 macOS 平台的 Adobe Acrobat DC（Classic 2015） 2015.006.30497 及之前版本
- 基于 macOS 平台的 Adobe Acrobat Reader DC（Continuous） 2019.012.20034 及之前版本
- 基于 macOS 平台的 Adobe Acrobat Reader DC（Classic 2017） 2017.011.30142 及之前版本
- 基于 macOS 平台的 Adobe Acrobat Reader DC（Classic 2015） 2015.006.30497 及之前版本
- 基于 Windows 平台的 Adobe Acrobat DC（Continuous） 2019.012.20035 及之前版本

- 基于 Windows 平台的 Adobe Acrobat DC（Classic 2017）2017.011.30143 及之前版本
- 基于 Windows 平台的 Adobe Acrobat DC（Classic 2015）2015.006.30498 及之前版本
- 基于 Windows 平台的 Acrobat Reader DC（Continuous）2019.012.20035 及之前版本
- 基于 Windows 平台的 Acrobat Reader DC（Classic 2017）2017.011.30143 及之前版本
- 基于 Windows 平台的 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

9. Microsoft Azure App Service on Azure Stack 缓冲区错误漏洞（CNNVD-201910-473）

Microsoft Azure App Service on Azure Stack 是美国微软（Microsoft）公司的一套平台即服务（PaaS）解决方案。该产品支持用户创建 Web、API 和 Azure Functions 应用等。

Microsoft Azure App Service on Azure Stack 中存在缓冲区错误漏洞，该漏洞源于程序在将内存复制到缓冲区时，没有检查缓冲区的长度。攻击者可利用该漏洞造成沙盒逃逸。

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-2019-1372

10. Cisco Aironet Access Points Software 访问控制错误漏洞（CNNVD-201910-1136）

Cisco Aironet 1540 Series APs 等都是美国思科（Cisco）公司的产品。Cisco Aironet 1540 Series APs 是一款 1540 系列访问接入点产品。Cisco Aironet 1560 Series APs 是一款 1560 系列访问接入点产品。Cisco Aironet 1800 Series APs 是一款 1800 系列访问接入点产品。Aironet Access Points（APs）Software 是运行在其中的一套操作系统。

Cisco APs Software 中存在访问控制错误漏洞，该漏洞源于程序没有对一些 URLs 进行充分的访问控制。远程攻击者可通过请求 URL 利用该漏洞以提升的权限未授权访问目标设备。以下产品及版本受到影响：

- Cisco Aironet 1540 Series APs
- Cisco Aironet 1560 Series APs
- Cisco Aironet 1800 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs
- Cisco Aironet 4800 APs

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-20191016-airo-unauth-access

11. qibosoft 代码注入漏洞（CNNVD-201910-947）

qibosoft 是中国齐博软件（qibosoft）公司的一套内容管理系统（CMS）。

qibosoft 7 版本中存在代码注入漏洞。该漏洞源于外部输入数据构造代码段的过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞生成非法的代码段，修改网络系统或组件的预期的执行控制流。

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：

http://www.qibosoft.com

12. Cisco Security Manager 代码问题漏洞（CNNVD-201910-143）

Cisco Security Manager（CSM）是美国思科（Cisco）公司的一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙、VPN 和入侵保护安全服务。

Cisco CSM 4.18 之前版本中的 Java 反序列化功能存在代码问题漏洞，该漏洞源于程序没有安全地反序列化用户提交的内容。攻击者可通过发送恶意的序列化 Java 对象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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-sm-java-deserial

13. Activesoft MyBuilder 操作系统命令注入漏洞（CNNVD-201910-243）

Activesoft MyBuilder 是韩国 Activesoft 公司的一款网页浏览器。ActiveX Control 是其中的一个 ActiveX 控件。

Activesoft MyBuilder 6.2.2019.814 之前版本中的 ActiveX Control 存在操作系统命令注入漏洞。攻击者可利用该漏洞执行任意命令。

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：

http://activesoft.co.kr

14. ZOHO ManageEngine OpManager SQL 注入漏洞（CNNVD-201910-937）

ZOHO ManageEngine OpManager 是美国卓豪（ZOHO）公司的一套网络、服务器及虚拟化监控软件。

ZOHO ManageEngine OpManager 12.4 build 124089 之前版本中存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 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/network-monitoring/help/read-me-complete.html

1.4.2 高危漏洞实例

本月高危漏洞共 581 个，其中重点漏洞实例如表 6 所示。

表 62019 年 10 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-201910-010	福昕	Adobe Acrobat 和 Reader 资源管理错误漏洞 (CNNVD-201910-884)
		CNNVD-201910-013		
		CNNVD-201910-016		
		CNNVD-201910-1301		

		CNNVD-201910-1303		
		CNNVD-201910-1314		
		CNNVD-201910-565	Siemens	
		CNNVD-201910-639		
		CNNVD-201910-1309	Mozilla	
		CNNVD-201910-596	Juniper Networks	
		CNNVD-201910-153		
		CNNVD-201910-784	ImageMagick Studio	
		CNNVD-201910-788		
		CNNVD-201910-748	Google	
		CNNVD-201910-752		
		CNNVD-201910-756		
		CNNVD-201910-762		
		CNNVD-201910-070	Cisco	
		CNNVD-201910-071		
		CNNVD-201910-834	Adobe	
		CNNVD-201910-835		
		CNNVD-201910-840		
		CNNVD-201910-847		
		CNNVD-201910-869		
		CNNVD-201910-878		
		CNNVD-201910-881		
		CNNVD-201910-884		
		CNNVD-201910-886		
		CNNVD-201910-888		
		CNNVD-201910-889		
		CNNVD-201910-890		
		CNNVD-201910-891		

		CNNVD-201910-896		
		CNNVD-201910-902		
		CNNVD-201910-910		
		CNNVD-201910-912		
2	注入	CNNVD-201910-420	IBM	IBM Spectrum Scale 注入漏洞(CNNVD-201910-420)
		CNNVD-201910-604	Palo Alto Networks	
3	信息泄露	CNNVD-201910-1024	Oracle	Oracle Fusion Middleware Business Intelligence Enterprise Edition 信息泄露漏洞(CNNVD-201910-1024)
		CNNVD-201910-1039		
		CNNVD-201910-1203	Trend Micro	
		CNNVD-201910-1208	中华电信	
		CNNVD-201910-1211		
		CNNVD-201910-1518	IBM	
		CNNVD-201910-476	Microsoft	
		CNNVD-201910-832	Adobe	
4	信任管理问题	CNNVD-201910-044	JetBrains	Palo Alto Networks Zingbox Inspector 信任管理问题漏洞(CNNVD-201910-605)
		CNNVD-201910-1074	Broadcom	
		CNNVD-201910-1137	CloudBees	
		CNNVD-201910-1228	Google	
		CNNVD-201910-566	Juniper Networks	
		CNNVD-201910-605	Palo Alto Networks	
		CNNVD-201910-608		
5	数字错误	CNNVD-201910-062	Cisco	Cisco Adaptive Security Appliance Software 和 Cisco Firepower Threat Defense 数字错误漏洞 (CNNVD-201910-062)
6	输入验证错误	CNNVD-201910-006	摩莎	IBM Security Directory Server 输入验证错误漏洞 (CNNVD-201910-018)
		CNNVD-201910-018	IBM	
		CNNVD-201910-1185	WordPress	

		CNNVD-201910-1204	Trend Micro	
		CNNVD-201910-1244		
		CNNVD-201910-255	SugarCRM	
		CNNVD-201910-261		
		CNNVD-201910-262		
		CNNVD-201910-263		
		CNNVD-201910-264		
		CNNVD-201910-265		
		CNNVD-201910-266		
		CNNVD-201910-267		
		CNNVD-201910-268		
		CNNVD-201910-269		
		CNNVD-201910-270		
		CNNVD-201910-271		
		CNNVD-201910-272		
		CNNVD-201910-787	Silicon Graphics	
		CNNVD-201910-641	NVIDIA	
		CNNVD-201910-1520	NetApp	
		CNNVD-201910-440	Microsoft	
		CNNVD-201910-454		
		CNNVD-201910-461		
		CNNVD-201910-564	Juniper Networks	
		CNNVD-201910-572		
		CNNVD-201910-575		
		CNNVD-201910-580		
		CNNVD-201910-583		
		CNNVD-201910-584		
		CNNVD-201910-590		

		CNNVD-201910-615		
		CNNVD-201910-041	JetBrains	
		CNNVD-201910-1175	ISC	
		CNNVD-201910-741	HP	
		CNNVD-201910-1222	Horner Automation	
		CNNVD-201910-1920	Honeywell	
		CNNVD-201910-1368	HAProxy	
		CNNVD-201910-031	Google	
		CNNVD-201910-1096		
		CNNVD-201910-190	Fon Wireless	
		CNNVD-201910-803	ESET	
		CNNVD-201910-1187	eQ-3	
		CNNVD-201910-061	Cisco	
		CNNVD-201910-079		
		CNNVD-201910-090		
		CNNVD-201910-098		
		CNNVD-201910-1116		
		CNNVD-201910-1138		
		CNNVD-201910-148		
		CNNVD-201910-149		
		CNNVD-201910-366	Centreon	
		CNNVD-201910-1300	Apache	
		CNNVD-201910-1442	Alfasado	
7	授权问题	CNNVD-201910-082	IBM	Microsoft Windows 和 Microsoft Windows Server 授权问题漏洞 (CNNVD-201910-438)
		CNNVD-201910-1186	eQ-3	
		CNNVD-201910-220	V-Zug	
		CNNVD-201910-381	Auth0	

		CNNVD-201910-438	Microsoft	
		CNNVD-201910-460		
		CNNVD-201910-571	Juniper Networks	
		CNNVD-201910-582		
		CNNVD-201910-609	Palo Alto Networks	
		CNNVD-201910-614	Magento	
		CNNVD-201910-841	Adobe	
8	路径遍历	CNNVD-201910-1437	小米科技	Adobe Acrobat 和 Reader 路径遍历漏洞(CNNVD-201910-1448)
		CNNVD-201910-1448	Adobe	
		CNNVD-201910-1557	Trend Micro	
		CNNVD-201910-1701	MikroTik	
		CNNVD-201910-195	Valve	
		CNNVD-201910-273	SugarCRM	
		CNNVD-201910-274		
		CNNVD-201910-282		
		CNNVD-201910-283		
		CNNVD-201910-718	IceWarp	
		CNNVD-201910-719		
9	跨站请求伪造	CNNVD-201910-1107	Cisco	Cisco 250 Series Smart Switches、350 Series Managed Switches 和 550X Series Stackable Managed Switches 跨站请求伪造漏洞(CNNVD-201910-1107)
		CNNVD-201910-1153	CloudBees	
		CNNVD-201910-1348		
		CNNVD-201910-1502	普联	
		CNNVD-201910-158	JetBrains	
10	跨站脚本	CNNVD-201910-1452	Red Hat	Juniper Networks Junos OS 跨站脚本漏洞(CNNVD-201910-563)
		CNNVD-201910-563	Juniper Networks	
11	竞争条件问题	CNNVD-201910-859	Adobe	Adobe Acrobat 和 Reader 竞争条件问题漏洞(CNNVD-201910-859)

12	加密问题	CNNVD-201910-1462	IBM	IBM Security Guardium Big Data Intelligence 加密问题漏洞 (CNNVD-201910-1519)
		CNNVD-201910-1519		
13	缓冲区错误	CNNVD-201910-011	福昕	Foxit Reader 缓冲区错误漏洞(CNNVD-201910-011)
		CNNVD-201910-015		
		CNNVD-201910-1290		
		CNNVD-201910-1306		
		CNNVD-201910-1313		
		CNNVD-201910-1224	Schneider Electric	
		CNNVD-201910-638	NVIDIA	
		CNNVD-201910-1310	Mozilla	
		CNNVD-201910-1321		
		CNNVD-201910-435	Microsoft	
		CNNVD-201910-447		
		CNNVD-201910-453		
		CNNVD-201910-455		
		CNNVD-201910-467		
		CNNVD-201910-470		
		CNNVD-201910-472		
		CNNVD-201910-477		
		CNNVD-201910-482		
		CNNVD-201910-487		
		CNNVD-201910-489		
		CNNVD-201910-491		
		CNNVD-201910-1174	Linux	
		CNNVD-201910-539	Intel	
		CNNVD-201910-789	ImageMagick Studio	
		CNNVD-201910-906	IBM	

		CNNVD-201910-1225	Horner Automation	
		CNNVD-201910-429	Google	
		CNNVD-201910-060	Cisco	
		CNNVD-201910-095		
		CNNVD-201910-097		
		CNNVD-201910-1115		
		CNNVD-201910-1117		
		CNNVD-201910-1119		
		CNNVD-201910-1120		
		CNNVD-201910-1121		
		CNNVD-201910-1123		
		CNNVD-201910-1124		
		CNNVD-201910-1126		
		CNNVD-201910-1127		
		CNNVD-201910-1129		
		CNNVD-201910-1130		
		CNNVD-201910-1132		
		CNNVD-201910-1133		
		CNNVD-201910-1680	Apache	
		CNNVD-201910-184		
		CNNVD-201910-836	Adobe	
		CNNVD-201910-850		
		CNNVD-201910-853		
		CNNVD-201910-858		
		CNNVD-201910-862		
		CNNVD-201910-864		
		CNNVD-201910-865		
		CNNVD-201910-866		

		CNNVD-201910-867		
		CNNVD-201910-868		
		CNNVD-201910-870		
		CNNVD-201910-873		
		CNNVD-201910-882		
		CNNVD-201910-885		
		CNNVD-201910-887		
		CNNVD-201910-893		
		CNNVD-201910-894		
		CNNVD-201910-897		
		CNNVD-201910-908		
		CNNVD-201910-909		
		CNNVD-201910-920		
14	后置链接	CNNVD-201910-1679	Apache	Apache Hadoop 后置链接漏洞(CNNVD-201910-1679)
		CNNVD-201910-466	Microsoft	
15	代码问题	CNNVD-201910-1558	Trend Micro	Adobe Acrobat 和 Reader 代码问题漏洞 (CNNVD-201910-851)
		CNNVD-201910-483	Microsoft	
		CNNVD-201910-191	Micro Focus	
		CNNVD-201910-493	Magento	
		CNNVD-201910-587	Juniper Networks	
		CNNVD-201910-040	JetBrains	
		CNNVD-201910-160		
		CNNVD-201910-275	Dell	
		CNNVD-201910-528	cPanel	
		CNNVD-201910-707	Cobham plc	
		CNNVD-201910-1417	Avast	
		CNNVD-201910-851	Adobe	
		CNNVD-201910-898		

		CNNVD-201910-899		
		CNNVD-201910-901		
16	操作系统命令注入	CNNVD-201910-099	Cisco	D-Link DBA-1510P 操作系统命令注入漏洞(CNNVD-201910-292)
		CNNVD-201910-157	JetBrains	
		CNNVD-201910-292	友讯	
		CNNVD-201910-724	仁宝电脑工业	
		CNNVD-201910-792	Centreon	
17	SQL 注入	CNNVD-201910-084	Cisco	Cisco Firepower Management Center SQL 注入漏洞(CNNVD-201910-086)
		CNNVD-201910-085		
		CNNVD-201910-086		
		CNNVD-201910-087		
		CNNVD-201910-089		
		CNNVD-201910-091		
		CNNVD-201910-093		
		CNNVD-201910-094		
		CNNVD-201910-606	Palo Alto Networks	
		CNNVD-201910-247	SugarCRM	
		CNNVD-201910-252		
		CNNVD-201910-253		
		CNNVD-201910-254		
		CNNVD-201910-256		
		CNNVD-201910-257		
		CNNVD-201910-258		
		CNNVD-201910-259		
		CNNVD-201910-260		
		CNNVD-201910-353	Netreo	
		CNNVD-201910-368	Centreon	

		CNNVD-201910-370		
		CNNVD-201910-520	Magento	
		CNNVD-201910-537		
		CNNVD-201910-1226	泛微	
		CNNVD-201910-647		

1. Adobe Acrobat 和 Reader 资源管理错误漏洞

(CNNVD-201910-884)

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 Reader 中存在资源管理错误漏洞。攻击者可利用该漏洞执行代码。基于 Windows 和 macOS 平台的以下产品及版本受到影响：

- Adobe Acrobat DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat 2015（Classic 2015）2015.006.30503 及之前版本
- Adobe Acrobat Reader DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat Reader 2017（Classic 2017）2017.011.30148 及之前版本

- Adobe Acrobat Reader 2015（Classic 2015）2015.006.30503 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/apsb19-49.html

2. IBM Spectrum Scale 注入漏洞(CNNVD-201910-420)

IBM Spectrum Scale 是美国 IBM 公司的一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。该产品支持帮助客户减少存储成本，同时提高云、大数据和分析环境中的安全性和管理效率等。

IBM Spectrum Scale 5.0.0.0 版本至 5.0.3.2 和 4.2.0.0 版本至 4.2.3.17 版本中存在注入漏洞。本地攻击者可利用该漏洞获取 root 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.ibm.com/support/pages/node/1073732

3. Oracle Fusion Middleware Business Intelligence Enterprise Edition 信息泄露漏洞(CNNVD-201910-1024)

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。Business Intelligence Enterprise Edition 是其中的一个为企业提供同类可视化分析和自助式发现平台的组件。

Oracle Fusion Middleware 中的 Business Intelligence Enterprise Edition 12.2.1.3.0 版本和 12.2.1.4.0 版本的 Installation 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/cpuoct2019-5072832.html

4. Palo Alto Networks Zingbox Inspector 信任管理问题漏洞 (CNNVD-201910-605)

Palo Alto Networks Zingbox Inspector 是美国 Palo Alto Networks 公司的一款 Zingbox IoT Command Center 物联网控制中心解决方案中的本地部署设备。

Palo Alto Networks Zingbox Inspector 1.294 及之前版本中存在信任管理问题漏洞。攻击者可利用该漏洞未授权访问系统。

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/170

5. Cisco Adaptive Security Appliance Software 和 Cisco Firepower Threat Defense 数字错误漏洞(CNNVD-201910-062)

Cisco Firepower Threat Defense（FTD）和 Cisco Adaptive Security Appliances Software（ASA Software）都是美国思科（Cisco）公司的产品。Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。该平台提供了对数据和网络资源的高度安全的访问等功能。

Cisco ASA Software 和 Cisco FTD 中的 SIP 检测模块存在数字错误漏洞，该漏洞源于程序没有正确解析 SIP 消息。远程攻击者可通

过发送恶意的 SIP 数据包利用该漏洞造成拒绝服务（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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-sip-dos

6. IBM Security Directory Server 输入验证错误漏洞 (CNNVD-201910-018)

IBM Security Directory Server 是美国 IBM 公司的一套使用了轻量级目录访问协议（LDAP）的企业身份管理软件。该软件提供一个可信的身份数据基础架构，用于身份验证。

IBM Security Directory Server 6.4.0 版本中存在输入验证错误漏洞。远程攻击者可通过诱使用户访问特制的网站利用该漏洞伪造 URL，进而获取敏感信息或实施其他攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/1077045

7. Microsoft Windows 和 Microsoft Windows Server 授权问题漏洞 (CNNVD-201910-438)

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 中存在授权问题漏洞，该漏洞源于程序没有正确处理身份验证请求。攻击者可通过运行特制的应用程序利用该漏洞以较高的权限执行任意代码。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 1809
- 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-2019-1322

8. Adobe Acrobat 和 Reader 路径遍历漏洞(CNNVD-201910-1448)

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 Reader 中存在路径遍历漏洞。攻击者可利用该漏洞泄露信息。基于 Windows 和 macOS 平台的以下产品及版本受到影响：

- Adobe Acrobat DC（Continuous）2019.010.20100 及之前版本
- Adobe Acrobat 2017（Classic 2017）2017.011.30140 及之前版本
- Adobe Acrobat DC（Classic 2015）2015.006.30495 及之前版本

- Adobe Acrobat Reader DC（Continuous）2019.010.20099 及之前版本
- Adobe Acrobat Reader 2017（Classic 2017）2017.011.30138 及之前版本
- Adobe Acrobat Reader DC（Classic 2015）2015.006.30493 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/apsb19-18.html

9. Cisco 250 Series Smart Switches、350 Series Managed Switches 和 550X Series Stackable Managed Switches 跨站请求伪造漏洞 (CNNVD-201910-1107)

Cisco 250 Series Smart Switches 等都是美国思科（Cisco）公司的产品。Cisco 250 Series Smart Switches 是一款 250 系列智能交换机。Cisco 350 Series Managed Switches 是一款 350 系列管理型交换机。550X Series Stackable Managed Switches 是一款 550X 系列管理型交换机。

Cisco 250 Series Smart Switches、350 Series Managed Switches 和 550X Series Stackable Managed Switches 中基于 Web 的管理界面存在跨站请求伪造漏洞，该漏洞源于程序没有进行充分的跨站请求伪造保护。远程攻击者可通过诱使该界面用户访问恶意的链接利用该漏洞以目标用户权限执行任意操作。

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-20191016-sbss-csrf

10. Juniper Networks Junos OS 跨站脚本漏洞(CNNVD-201910-563)

Juniper Networks Junos OS 是美国瞻博网络（Juniper Networks）公司的一套专用于该公司的硬件设备的网络操作系统。该操作系统提供了安全编程接口和 Junos SDK。

Juniper Networks Junos OS 中的 J-Web 界面存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。以下产品及版本受到影响：

- Juniper Networks Junos OS 12.1X46 版本
- Juniper Networks Junos OS 12.3 版本
- Juniper Networks Junos OS 12.3X48 版本
- Juniper Networks Junos OS 14.1X53 版本
- Juniper Networks Junos OS 15.1 版本
- Juniper Networks Junos OS 15.1X49 版本
- Juniper Networks Junos OS 15.1X53 版本
- Juniper Networks Junos OS 16.1 版本
- Juniper Networks Junos OS 16.2 版本
- Juniper Networks Junos OS 17.1 版本
- Juniper Networks Junos OS 17.2 版本
- Juniper Networks Junos OS 17.3 版本
- Juniper Networks Junos OS 17.4 版本

- Juniper Networks Junos OS 18.1 版本
- Juniper Networks Junos OS 18.2 版本
- Juniper Networks Junos OS 18.3 版本
- Juniper Networks Junos OS 18.4 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://kb.juniper.net/InfoCenter/index?page=content&id=JSA10970&actp=METADATA

11. Adobe Acrobat 和 Reader 竞争条件问题漏洞

(CNNVD-201910-859)

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 Reader 中存在竞争条件问题漏洞。攻击者可利用该漏洞执行代码。基于 Windows 和 macOS 平台的以下产品及版本受到影响：

- Adobe Acrobat DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat 2015（Classic 2015）2015.006.30503 及之前版本
- Adobe Acrobat Reader DC（Continuous）2019.012.20040 及之前版本

- Adobe Acrobat Reader 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat Reader 2015（Classic 2015）2015.006.30503 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/apsb19-49.html

12. IBM Security Guardium Big Data Intelligence 加密问题漏洞 (CNNVD-201910-1519)

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 (SonarG) 4.0 版本中存在加密问题漏洞，该漏洞源于程序使用了较弱的加密算法。攻击者可利用该漏洞解密敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/1096924

13. Foxit Reader 缓冲区错误漏洞(CNNVD-201910-011)

Foxit Reader 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。

Foxit Reader 9.6.0.25114 及之前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，补丁获取链接：

https://www.foxitsoftware.com/support/security-bulletins.php

14. Apache Hadoop 后置链接漏洞(CNNVD-201910-1679)

Apache Hadoop 是美国阿帕奇（Apache）软件基金会的一套开源的分布式系统基础架构。该产品能够对大量数据进行分布式处理，并具有高可靠性、高扩展性、高容错性等特点。

Apache Hadoop 1.0.3 版本中存在后置链接漏洞。本地攻击者可利用该漏洞获取提升的权限。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://hadoop.apache.org

15. Adobe Acrobat 和 Reader 代码问题漏洞(CNNVD-201910-851)

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 Reader 中存在代码问题漏洞。攻击者可利用该漏洞执行代码。基于 Windows 和 macOS 平台的以下产品及版本受到影响：

- Adobe Acrobat DC（Continuous）2019.012.20040 及之前版本
- Adobe Acrobat 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat 2015（Classic 2015）2015.006.30503 及之前版本
- Adobe Acrobat Reader DC（Continuous）2019.012.20040 及之前版本

- Adobe Acrobat Reader 2017（Classic 2017）2017.011.30148 及之前版本
- Adobe Acrobat Reader 2015（Classic 2015）2015.006.30503 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/apsb19-49.html

16. D-Link DBA-1510P 操作系统命令注入漏洞

(CNNVD-201910-292)

D-Link DBA-1510P 是中国台湾友讯（D-Link）公司的一款无线接入点设备。

使用 1.70b009 及之前版本固件的 D-Link DBA-1510P 中的 Web User Interface 存在操作系统命令注入漏洞。攻击者可利用该漏洞执行任意的操作系统命令。

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

17. Cisco Firepower Management Center SQL 注入漏洞

(CNNVD-201910-086)

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。

Cisco FMC 中的基于 Web 的管理界面存在 SQL 注入漏洞，该漏洞源于程序没有进行正确的输入验证。远程攻击者可通过发送特制的 SQL 查询利用该漏洞查看信息并在底层操作系统中执行命令。以下产

品及版本受到影响：

- Cisco FMC 6.0.0 版本
- Cisco FMC 6.2.0 版本
- Cisco FMC 6.2.1 版本
- Cisco FMC 6.2.2 版本

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj

二、接报漏洞情况

本月接报漏洞共计 12164 个，其中信息技术产品漏洞（通用型漏洞）104 个，网络信息系统漏洞（事件型漏洞）12060 个。

表 7 2019 年 10 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	网神信息技术（北京）股份有限公司	8666	0	8666
2	上海斗象信息科技有限公司	2860	2	2860
3	四川虹微技术有限公司子午攻防实验室	157	0	157
4	西安四叶草信息技术有限公司	117	0	117
5	山东新潮信息技术有限公司	56	1	55
6	北京圣溥润高新技术服份有限公司	40	0	40
7	上海安洵信息技术有限公司	35	0	35

8	内蒙古奥创科技有限公司	33	22	11
9	北京数字观星科技有限公司	30	0	30
10	河南听潮盛世信息技术有限公司	29	0	29
11	北京天融信网络安全技术有限公司	26	26	0
12	北京华云安信息技术有限公司	22	0	22
13	广州锦行网络科技有限公司	20	0	20
14	北京神州绿盟科技有限公司安全研究部	14	14	0
15	梆梆安全	12	12	0
16	太极计算机股份有限公司	11	0	11
17	上海安识网络科技有限公司	8	4	4
18	国发中新（北京）科技发展有限公司	5	0	5
19	个人	4	4	0
20	广州竞远安全技术股份有限公司	4	4	0
21	北京智游网安科技有限公司	2	2	0
22	哈尔滨安天科技股份有限公司	2	2	0
23	北京智游网安科技有限公司	2	2	0
24	上海三零卫士信息安全有限公司	2	2	0
25	中兴通讯	2	2	0
26	厦门服云信息科技有限公司	1	1	0
27	MS17-010 安全实验室	1	1	0
28	北京威努特技术有限公司	1	1	0
29	哈尔滨安天科技股份有限公司	1	1	0

30	众安天下	1	1	0
报送总计		12164	104	12060

三、重大漏洞预警

3.1 关于 Oracle WebLogic Server 反序列化漏洞的预警

本月，国家信息安全漏洞库（CNNVD）收到 Oracle WebLogic Server 反序列化漏洞（CNNVD-201910-1034、CVE-2019-2890）（CNNVD-201910-1035、CVE-2019-2887）情况的报送。攻击者可利用该漏洞在未授权的情况下发送攻击数据,最终实现远程代码执行。WebLogic Server 10.3.6.0、12.1.3.0、12.2.1.3 等版本均受漏洞影响。目前， Oracle 官方已经发布补丁修复了漏洞，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

Oracle WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

Weblogic 中的序列化是指把 Java 对象转换为字节序列的过程便于保存在内存、文件、数据库中，反序列化是指把字节序列恢复为 Java 对象的过程。

Weblogic 在利用 T3 协议进行远程资源加载调用时，默认会进行黑名单过滤以保证反序列化安全。攻击者可利用漏洞绕过 Weblogic 反序列化黑名单，在未授权的情况下发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行，进而

控制 WebLogic 服务器。

漏洞危害

攻击者可利用漏洞在未授权的情况下发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行。该漏洞涉及了多个版本，具体受影响版本如下：

Oracle WebLogic Server 10.3.6.0
Oracle WebLogic Server 12.1.3.0
Oracle WebLogic Server 12.2.1.3

修复措施

目前， Oracle 官方已经发布补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。Oracle 官方更新链接如下：

https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

3.2 关于泛微 E-cology OA 系统 SQL 注入漏洞的预警

本月，国家信息安全漏洞库（CNNVD）收到关于泛微 E-cology OA 系统 SQL 注入漏洞（CNNVD-201910-1226）情况的报送。2019 年 10 月 17 日，泛微 e-cology OA 发布了安全更新补丁，修复了 SQL 注入相关漏洞，这次是在 10 月 10 日发布的 SQL 注入漏洞补丁后更新发布的最新漏洞补丁。成功利用此漏洞的攻击者，可以远程获取目标系

统的数据库敏感信息。泛微 E-cology OA V9 V8 版本均受此漏洞影响。目前，泛微官方已发布漏洞补丁，请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

泛微 E-cology OA 系统是一套兼具企业信息门户、知识管理、数据中心、工作流管理、人力资源管理、客户与合作伙伴管理、项目管理、财务管理、资产管理功能的协同商务平台。泛微 e-cology OA 系统存在 SQL 查询语句过滤不严的情况(直接语句拼接)，从而导致 SQL 注入漏洞，恶意攻击者可以通过构造恶意查询语句的攻击代码触发漏洞，利用该漏洞可以获取数据库中敏感信息。

通过对泛微 E-cology OA 系统在互联网中的 IP 地址进行分析，2019 年全球共 19389 个用户联网使用该系统，主要用户分布在中国，共 19040 个，其中北京地区用户量最多，共 4379 个。目前，该漏洞利用 poc 已经在网络中流传，存在较大风险，建议用户及时采取解决措施。

漏洞危害

成功利用此漏洞的攻击者，可以远程获取目标系统的数据库敏感信息。泛微 E-cology OA V9 V8 版本均受此漏洞影响。

安全建议

目前，泛微官方已发布漏洞补丁，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方补丁地址如下：

https://www.weaver.com.cn/cs/securityDownload.asp