北京师范大学网络信息安全通告

2020 年 3 月报告

北京师范大学信息网络中心

2020 年 4 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，2020 年 3 月份新增安全漏洞共 1726 个，从厂商分布来看，Samsung 公司产品的漏洞数量最多，共发布 123 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 15.47%。本月新增漏洞中，超危漏洞 293 个、高危漏洞 677 个、中危漏洞 705 个、低危漏洞 51 个，相应修复率分别为 72.70%、82.72%、69.65%以及 86.27%。合计 1308 个漏洞已有修复补丁发布，本月整体修复率 75.78%。

截至 2020 年 03 月 31 日，CNNVD 采集漏洞总量已达 142115 个。

1.1 漏洞增长概况

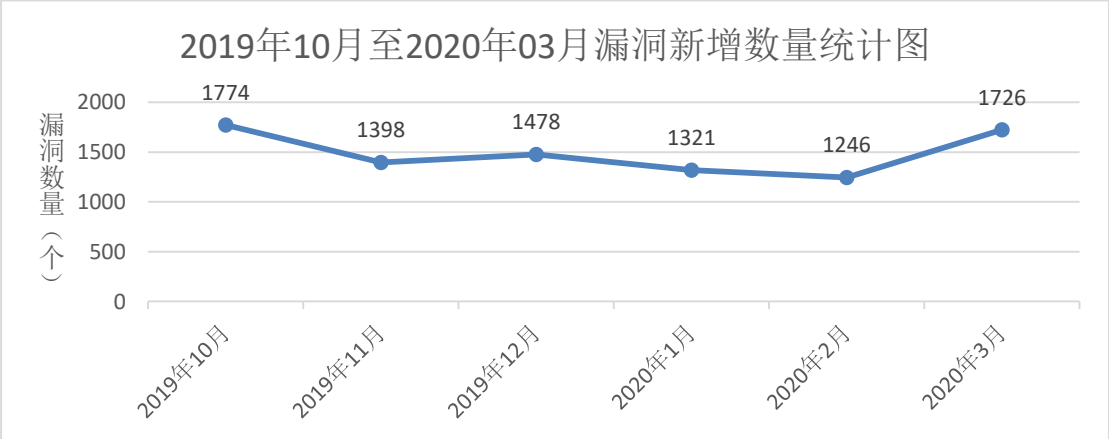

图 1 2019 年 9 月至 2020 年 3 月漏洞新增数量统计图

2020 年 3 月新增安全漏洞 1726 个，与上月（1246 个）相比增加了 38.52%。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 1491 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

3 月厂商漏洞数量分布情况如表 1 所示，Samsung 公司漏洞达到 123 个，占本月漏洞总量的 7.13%。本月 Microsoft、Google 等厂商的漏洞数量出现较不同程度的下降。

表 1　2020 年 3 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	Samsung	123	7.13%
2	Microsoft	117	6.78%
3	Google	64	3.71%
4	Qualcomm	48	2.78%
5	Apple	46	2.67%
6	Adobe	42	2.43%
7	GitLab	41	2.38%
8	IBM	40	2.32%
9	CloudBees	38	2.20%
10	Intel	27	1.56%

1.2.2 漏洞产品分布

3 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 10 漏洞数量最多，共 80 个，占主流操作系统漏洞总量的 12.82%，排名第一。

表 2　2020 年 3 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Windows 10	80
2	Windows Server 2019	72
3	Windows Server 2016	72
4	Windows Server 2012	56
5	Windows 8.1	56
6	Windows Server 2012 R2	56
7	Windows Rt 8.1	56
8	Android	52
9	Windows 7	40
10	Windows Server 2008	40
11	Windows Server 2008 R2	40
12	Linux Kernel	4

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3 漏洞类型分布

3 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 15.47%。

表 3 2020 年 3 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	跨站脚本	267	15.47%
2	缓冲区错误	265	15.35%
3	信息泄露	118	6.84%
4	代码问题	110	6.37%
5	输入验证错误	105	6.08%
6	资源管理错误	57	3.30%
7	SQL 注入	56	3.24%
8	跨站请求伪造	55	3.19%
9	操作系统命令注入	54	3.13%
10	授权问题	52	3.01%
11	注入	42	2.43%

12	路径遍历	35	2.03%
13	访问控制错误	22	1.27%
14	代码注入	20	1.16%
15	信任管理问题	16	0.93%
16	竞争条件问题	12	0.70%
17	加密问题	8	0.46%
18	环境问题	6	0.35%
19	数据伪造问题	5	0.29%
20	日志信息泄露	5	0.29%
21	后置链接	4	0.23%
22	安全特征问题	3	0.17%
23	数字错误	3	0.17%
24	命令注入	2	0.12%
25	权限许可和访问控制问题	2	0.12%
26	格式化字符串错误	1	0.06%
27	参数注入	1	0.06%
28	其他	400	23.17%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。3 月漏洞危害等级分布如图 2 所示，其中超危漏洞 293 条，占本月漏洞总数的 16.98%。

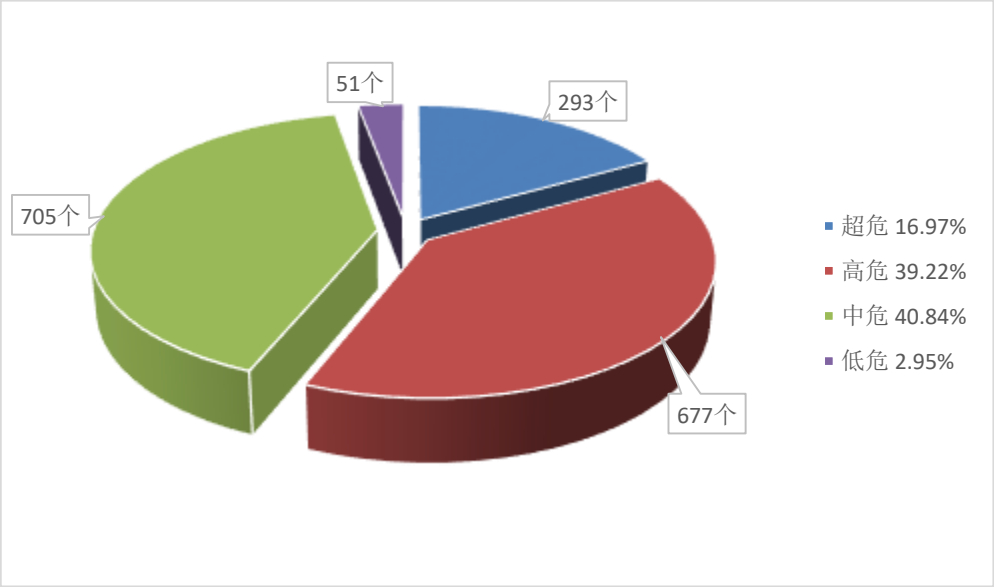

图 2　2020 年 3 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

3 月漏洞修复情况按危害等级进行统计见图 3。其中低危漏洞修复率最高，达到 86.27%，中危漏洞修复率最低，比例为 69.65%。总体来看，本月整体修复率，由上月的 74.88%上升至本月的 75.78%。

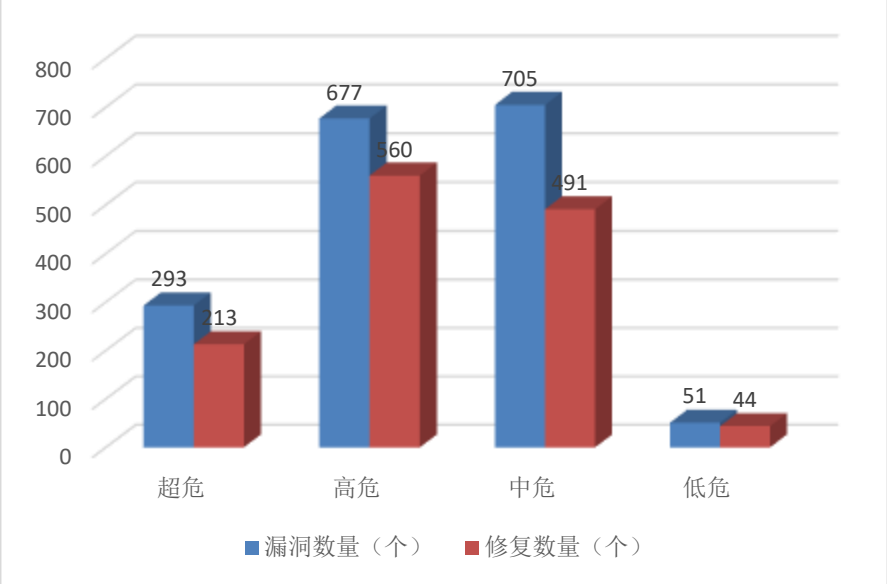

图 3　2020 年 3 月漏洞修复数量统计

1.3.2　厂商修复情况

3 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Samsung、Microsoft、Google 等十个厂商共 586 条漏洞，占本月漏洞总数的 33.95%，漏洞修复率为 98.98%，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 Samsung、Google、Qualcomm、Apple、Adobe、GitLab、IBM、CloudBees 等公司本月漏洞修复率均为 100%，共 580 条漏洞已全部修复。

表 4　2020 年 3 月厂商修复情况统计表

序号	厂商名称	漏洞数量（个）	修复数量	修复率
1	Samsung	123	123	100.00%
2	Microsoft	117	116	99.15%
3	Google	64	64	100.00%
4	Qualcomm	48	48	100.00%
5	Apple	46	46	100.00%
6	Adobe	42	42	100.00%
7	GitLab	41	41	100.00%
8	IBM	40	40	100.00%
9	CloudBees	38	38	100.00%
10	Intel	27	22	81.48%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 293 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 3 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	缓冲区错误	CNNVD-202003-612	Mozilla 基金会	Adobe Acrobat 和 Reader 缓冲区错误漏洞（CNNVD-202003-1043）
		CNNVD-202003-1043	Adobe	
		CNNVD-202003-1388	Samsung	
		CNNVD-202003-1388		
		CNNVD-202003-1392		
2	环境问题	CNNVD-202003-1353	Apache 软件基金会	Apache Traffic Server 环境问题漏洞（CNNVD-202003-1353）
		CNNVD-202003-1355		
3	跨站脚本	CNNVD-202003-028	NETGEAR	Microsoft Application Inspector 跨站脚本漏洞（CNNVD-202003-520）
		CNNVD-202003-379	LiveZilla	
		CNNVD-202003-520	Microsoft	
		CNNVD-202003-873	Dell	
4	授权问题	CNNVD-202003-191	HUMAX	Apache Shiro 授权问题漏洞（CNNVD-202003-1579）
		CNNVD-202003-200		
		CNNVD-202003-1025	cPanel	
		CNNVD-202003-1160	Opera	

		CNNVD-202003-1161	Software	
		CNNVD-202003-1579	Apache 软件基金会	
5	输入验证错误	CNNVD-202003-124	Qualcomm	Microsoft Server Message Block 安全漏洞（CNNVD-202003-607）
		CNNVD-202003-215	ESET	
		CNNVD-202003-311	WAGO	
		CNNVD-202003-503	Johnson Controls	
		CNNVD-202003-821	Apache 软件基金会	
		CNNVD-202003-928	Google	
		CNNVD-202003-1087	Adobe	
		CNNVD-202003-607	Microsoft	
		CNNVD-202003-1434	Samsung	
6	资源管理错误	CNNVD-202003-1047	Adobe	Adobe Acrobat 和 Reader 资源管理错误漏洞（CNNVD-202003-1047）
		CNNVD-202003-1048		
		CNNVD-202003-1052		
		CNNVD-202003-1062		
		CNNVD-202003-1448	Samsung	
7	路径遍历	CNNVD-202003-873	SAP	Safescan Timemoto TA-8000 系列路径遍历漏洞（CNNVD-202003-826）
		CNNVD-202003-588	Safescan	
		CNNVD-202003-826	Trend Micro	
		CNNVD-202003-1008	NETSAS	
		CNNVD-202003-1198	VISAM	
		CNNVD-202003-1521	SAP	
8	其他	CNNVD-202003-049	Dell	Microsoft DirectX 安全漏洞（CNNVD-202003-603）
		CNNVD-202003-614	Technicolor	
		CNNVD-202003-618	Sumavision	
		CNNVD-202003-783	OpenStack MediaWiki 基金会	
		CNNVD-202003-810		
		CNNVD-202003-845	GitLab	
		CNNVD-202003-867	RICOH	
		CNNVD-202003-906	Meetecho	
		CNNVD-202003-1002	Mitsubishi	
		CNNVD-202003-1028	cPanel	
		CNNVD-202003-1077	Adobe	
		CNNVD-202003-603	Microsoft	
		CNNVD-202003-1380	Samsung	

1. Adobe Acrobat 和 Reader 缓冲区错误漏洞（CNNVD-202003-1043）

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。

- 基于 Windows 和 macOS 平台的 Adobe Acrobat 和 Reader 中存在缓冲区错误漏洞。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：Adobe Acrobat DC（Continuous）2020.006.20034 及之前版本，Acrobat 2017（Classic 2017）2017.011.30158 及之前版本，Acrobat 2015（Classic 2015）2015.006.30510 及之前版本；Acrobat Reader DC（Continuous）2020.006.20034 及之前版本，Acrobat Reader 2017（Classic 2017）2017.011.30158 及之前版本，Acrobat Reader 2015（Classic 2015）2015.006.30510 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/apsb20-13.html

2. Apache Traffic Server 环境问题漏洞（CNNVD-202003-1353）

Apache Traffic Server（ATS）是美国阿帕奇（Apache）软件基金会的一套可扩展的 HTTP 代理和缓存服务器。

Apache Traffic Server 6.0.0 版本至 6.2.3 版本、7.0.0 版本至 7.1.8 版本和 8.0.0 版本至 8.0.5 版本中存在环境问题漏洞，该漏洞源于不正确的输入验证。攻击者可借助特制的请求利用该漏洞实施 HTTP 请求夹带攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/r99d18d0bc4daa05e7d0e5a63e0e22701a421b2ef5a8f4f7694c43869%40%3Cannounce.trafficserver.apache.org%3E

3. Microsoft Application Inspector 跨站脚本漏洞（CNNVD-202003-520）

Microsoft Application Inspector 是美国微软（Microsoft）公司的一款软件源代码分析工具。该产品支持扫描 C、C++、C＃、Java 和 JavaScript 等多种语言。

Microsoft Application Inspector v1.0.23 及之前版本中存在远程代码问题漏洞。攻击者可利用该漏洞将代码段发送到外部服务器上。

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-2020-0872

4. Apache Shiro 授权问题漏洞（CNNVD-202003-1579）

Apache Shiro 是美国阿帕奇（Apache）软件基金会的一套用于执行认证、授权、加密和会话管理的 Java 安全框架。

Apache Shiro 1.5.2 之前版本中存在安全漏洞。攻击者可借助特制的请求利用该漏洞绕过身份验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/rc64fb2336683feff3580c3c3a8b28e80525077621089641f2f386b63@%3Ccommits.camel.apache.org%3E

5. Microsoft Server Message Block 安全漏洞（CNNVD-202003-607）

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。Server Message Block 是其中的一个服务器信息传输协议。

Microsoft Server Message Block 3.1.1 (SMBv3)版本中存在安全漏洞，该漏洞源于 SMBv3 协议在处理恶意压缩数据包时，进入了错误流程。远程未经身份验证的攻击者可利用该漏洞在应用程序中执行任意代码。以下产品及版本受到影响：Microsoft Windows 10 版本 1903，Windows Server 版本 1903，Windows 10 版本 1909，Windows Server 版本 1909。

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-2020-0796

6. Adobe Acrobat 和 Reader 资源管理错误漏洞（CNNVD-202003-1047）

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。

基于 Windows 和 macOS 平台的 Adobe Acrobat 和 Reader 中存在安全漏洞。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：Adobe Acrobat DC（Continuous）2020.006.20034 及之前版本，Acrobat 2017（Classic 2017）2017.011.30158 及之前版本，Acrobat 2015

（Classic 2015）2015.006.30510 及之前版本；Acrobat Reader DC（Continuous）2020.006.20034 及之前版本，Acrobat Reader 2017（Classic 2017）2017.011.30158 及之前版本，Acrobat Reader 2015（Classic 2015）2015.006.30510 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/apsb20-13.html

7. Safescan Timemoto TA-8000 系列路径遍历漏洞（CNNVD-202003-826）

Safescan Timemoto TA-8000 是荷兰 Safescan 公司的一套 TA-8000 系列考勤系统。

Safescan Timemoto TA-8000 系列 1.0 版本中存在路径遍历漏洞。远程攻击者可借助用于管理 API 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://support.timemoto.com/en/s/safescan-time-clock-systems/a/firmware-update-7-dot-03-dot-100-ta8000-14

8. Microsoft DirectX 安全漏洞（CNNVD-202003-603）

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。DirectX 是其中的一个多媒体系统链接库。

Microsoft DirectX 中存在安全漏洞，该漏洞源于程序没有正确地处理内存对象。攻击者可通过登录到系统并运行特制的应用程序利用

该漏洞在内核模式中运行任意代码。以下产品及版本受到影响：Microsoft Windows 10，Windows 10 Version 1607，Windows 10 版本 1709，Windows 10 版本 1803，Windows 10 版本 1809，Windows 10 版本 1903，Windows 10 版本 1909，Windows Server 2016，Windows Server 版本 1803，Windows Server 版本 1903，Windows Server 版本 1909。

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-2020-0690

1.4.2 高危漏洞实例

本月高危漏洞共 677 个，其中重点漏洞实例如表 6 所示。

表 6 2020 年 3 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202003-198	Sympa	Cisco SD-WAN Solution vManage SQL 注入漏洞（CNNVD-202003-1140）
		CNNVD-202003-1140	Siemens	
		CNNVD-202003-1441	Qualcomm	
		CNNVD-202003-1442		
		CNNVD-202003-1465		
		CNNVD-202003-198	TestLink	
		CNNVD-202003-1466	Samsung	
		CNNVD-202003-1488		
		CNNVD-202003-770	RegistrationMagic	
		CNNVD-202003-881	Thoughtbot	
		CNNVD-202003-945	Dolibarr 基金会	
2	操作系统命令注入	CNNVD-202003-154	Symantec	IBM Spectrum Scale 和 IBM Spectrum Protect Plus 操作系统命令注入漏洞（CNNVD-202003-1688
		CNNVD-202003-201	Druva	
		CNNVD-202003-1688	D-Link	
		CNNVD-202003-258		
		CNNVD-202003-259		

		CNNVD-202003-265	IBM	）
		CNNVD-202003-1693	CloudBees	
		CNNVD-202003-289	Vesta Control Panel	
		CNNVD-202003-1606	TP-Link	
		CNNVD-202003-1610		
3	代码问题	CNNVD-201708-170	IDM Computer Solutions	Intel Graphics Drivers 代码问题漏洞（CNNVD-202003-533）
		CNNVD-202003-127	Qualcomm	
		CNNVD-202003-138		
		CNNVD-202003-213	Red Software	
		CNNVD-202003-290	CloudBees	
		CNNVD-202003-314		
		CNNVD-202003-322		
		CNNVD-202003-332	BookStack	
		CNNVD-202003-342	Widget Factory	
		CNNVD-202003-349	Joobi	
		CNNVD-202003-361	Lexmark	
		CNNVD-202003-267	IBM	
		CNNVD-202003-1358	IBM	
		CNNVD-202003-1476	Samsung	
		CNNVD-202003-1477	Samsung	
		CNNVD-202003-533	Intel	
4	缓冲区错误	CNNVD-202003-077	Google	Microsoft Internet Explorer 缓冲区错误漏洞（CNNVD-202003-388）
		CNNVD-202003-058		
		CNNVD-202003-073		
		CNNVD-202003-102	Qualcomm	
		CNNVD-202003-104		
		CNNVD-202003-106		
		CNNVD-202003-146	Facebook	
		CNNVD-202003-147		
		CNNVD-202003-148		
		CNNVD-202003-388	Microsoft	
		CNNVD-202003-390		
		CNNVD-202003-399		
		CNNVD-202003-400		
		CNNVD-202003-401		
		CNNVD-202003-414		
		CNNVD-202003-981	Foxit	
		CNNVD-202003-987		
		CNNVD-202003-994		
		CNNVD-202003-1113	Cisco	
		CNNVD-202003-1411	Samsung	

		CNNVD-202003-1444		
		CNNVD-202003-1478		
		CNNVD-202003-1544	Apple	
		CNNVD-202003-1545		
		CNNVD-202003-1547		
		CNNVD-202003-1569		
5	跨站请求伪造	CNNVD-202003-182	Cisco	Cisco Prime Network Registrar 跨站请求伪造漏洞（CNNVD-202003-182）
		CNNVD-202003-1700	IBM	
		CNNVD-202003-818	Untis	
		CNNVD-202003-908	OnTheGoSystems	
		CNNVD-202003-956	Nagios	
		CNNVD-202003-1229	Canon	
		CNNVD-202003-1234	NETSAS	
		CNNVD-202003-1590	CloudBees	
		CNNVD-202003-1674	Lenovo	
6	路径遍历	CNNVD-202003-402	Lexmark	Intel Graphics Drivers 路径遍历漏洞（CNNVD-202003-537）
		CNNVD-202003-537	Intel	
		CNNVD-202003-857	Kyocera	
		CNNVD-202003-1338	Schneider Electric	
		CNNVD-202003-1652	GitLab	
		CNNVD-202003-1673	Lenovo	
7	资源管理错误	CNNVD-202003-103	Qualcomm	多款 Apple 产品 WebKit 组件资源管理错误漏洞（CNNVD-202003-1546）
		CNNVD-202003-108		
		CNNVD-202003-117		
		CNNVD-202003-889	VMware	
		CNNVD-202003-1051	Adobe	
		CNNVD-202003-1203	Hancom	
		CNNVD-202003-1179	Google	
		CNNVD-202003-1188		
		CNNVD-202003-1195		
		CNNVD-202003-1651	GitLab	
		CNNVD-202003-490	Mozilla 基金会	
		CNNVD-202003-989	Foxit	
		CNNVD-202003-1401	Samsung	
		CNNVD-202003-1546	Apple	
8	代码注入	CNNVD-202003-1130	Dell	Cisco Data Center Network Manager 权限许可和访问控制问题漏洞
		CNNVD-202003-600	SAP	
		CNNVD-202003-1317	Eaton	

		CNNVD-202003-1352	Ansible	（CNNVD-202002-975）

1. Cisco SD-WAN Solution vManage SQL 注入漏洞（CNNVD-202003-1140）

Cisco SD-WAN Solution 是美国思科（Cisco）公司的一套网络扩展解决方案。vManage 是一套网络管理系统。

Cisco SD-WAN Solution vManage Release 19.2.2 之前版本中的 Web UI 存在 SQL 注入漏洞，该漏洞源于 Web UI 没有正确验证 SQL 值。远程攻击者可通过进行身份验证并发送恶意的 SQL 值利用该漏洞修改底层数据库和操作系统上的值或返回值。

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-20200318-vmanage-cypher-inject

2. IBM Spectrum Scale 和 IBM Spectrum Protect Plus 操作系统命令注入漏洞（CNNVD-202003-1688）

IBM Spectrum Scale 和 IBM Spectrum Protect Plus 都是美国 IBM 公司的产品。IBM Spectrum Scale 是一套基于 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 Protect Plus 是一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。

IBM Spectrum Scale 和 IBM Spectrum Protect Plus 10.1.0 版本

至 10.1.5 版本中存在操作系统命令注入漏洞。远程攻击者可通过发送特制的请求利用该漏洞在系统上中执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/6114130

3. Intel Graphics Drivers 代码问题漏洞（CNNVD-202003-533）

Intel Graphics Drivers 是美国英特尔（Intel）公司的一款集成显卡驱动程序。

Intel Graphics Drivers 26.20.100.7158 之前版本中存在安全漏洞。本地攻击者可利用该漏洞提升权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00315.html

4. Microsoft Internet Explorer 缓冲区错误漏洞（CNNVD-202003-388）

Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。

- Microsoft IE 11 中脚本引擎处理内存对象的方式存在远程代码执行漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码，损坏内存。

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-2020-0833

5. Cisco Prime Network Registrar 跨站请求伪造漏洞（CNNVD-202003-182）

Cisco Prime Network Registrar（CPNR）是美国思科（Cisco）公司的一款网络注册器产品。该产品提供了动态主机配置协议（DHCP）、域名系统（DNS）和 IP 地址管理（IPAM）等服务。

Cisco CPNR 10.1 之前版本（releases）中基于 Web 的接口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用户点击恶意链接利用该漏洞修改设备配置，进而可以编辑或创建任意权限用户的账户。

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-cpnr-csrf-WWTrDkyL

6. Intel Graphics Drivers 路径遍历漏洞（CNNVD-202003-537）

Intel Graphics Drivers 是美国英特尔（Intel）公司的一款集成显卡驱动程序。

Intel Graphics Drivers 中的 igdkmd64.sys 文件存在路径遍历漏洞。本地攻击者可利用该漏洞提升权限。以下产品及版本受到影响：Intel Graphics Drivers 15.45.30.5103 之前版本，15.40.44.5107 之前版本，15.36.38.5117 之前版本，15.33.49.5100 之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00315.html

7. 多款 Apple 产品 WebKit 组件资源管理错误漏洞

（CNNVD-202003-1546）

Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Web Kit 是其中的一个 Web 浏览器引擎组件。

多款 Apple 产品中的 WebKit 组件存在资源管理错误漏洞。攻击者可借助恶意制作的 Web 内容利用该漏洞执行代码。以下产品及版本受到影响：基于 Windows 平台的 Apple iCloud 7.18 之前版本，10.9.3 之前版本；基于 Windows 平台的 iTunes 12.10.5 之前版本；iOS 13.4 之前版本；iPadOS 13.4 之前版本；Safari 13.1 之前版本；tvOS 13.4 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://support.apple.com/zh-cn/HT211101

https://support.apple.com/zh-cn/HT211102

https://support.apple.com/zh-cn/HT211104

https://support.apple.com/zh-cn/HT211105

https://support.apple.com/zh-cn/HT211106

https://support.apple.com/zh-cn/HT211107

8. Dell EMC Data Protection Advisor 代码注入漏洞

（CNNVD-202003-1130）

Dell EMC Data Protection Advisor 是美国戴尔（Dell）公司的一

套数据保护管理解决方案。该方案支持自动和集中执行所有此类数据的收集与分析，并获得数据保护环境和活动的单个全面视图等。

Dell EMC Data Protection Advisor 中的 REST API 存在代码注入漏洞。远程攻击者可借助特制脚本利用该漏洞在系统上执行任意命令。以下产品及版本受到影响：Dell EMC Data Protection Advisor 6.3 版本，6.4 版本，6.5 版本，18.2 版本，19.1 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://www.dell.com/support/security/zh-cn/details/539430/DSA-2019-155-Dell-EMC-Data-Protection-Advisor-Security-Update-for-Multiple-Vulnerabilities

二、接报漏洞情况

本月接报漏洞 7156 个，其中信息技术产品漏洞（通用型漏洞）217 个，网络信息系统漏洞（事件型漏洞）6939 个。

表 7 2020 年 3 月漏洞接报情况

序号	报送单位	漏洞总量
1	网神信息技术（北京）股份有限公司	3025
2	上海斗象信息科技有限公司	2963
3	北京华云安信息技术有限公司	411
4	太极计算机股份有限公司	250
5	西安四叶草信息技术有限公司	80
6	北京国舜科技股份有限公司	65
7	中国电信集团系统集成有限责任公司	45

8	北京启明星辰信息安全技术有限公司	41
9	内蒙古洞明科技有限公司	40
10	北京圣溥润高新技术服份有限公司	37
11	山东新潮信息技术有限公司	25
12	浙江大华技术股份有限公司	19
13	上海安洵信息技术有限公司	18
14	北京数字观星科技有限公司	16
15	北京云测信息技术有限公司	13
16	恒安嘉新（北京）科技股份公司	9
17	北京梆梆安全科技有限公司	8
18	北京神州绿盟科技有限公司	8
19	北京山石网科信息技术有限公司	8
20	西安交大捷普网络科技有限公司	8
21	中新网络信息安全股份有限公司	6
22	浙江宇视科技有限公司	6
23	天津市兴先道科技有限公司	6
24	河南听潮盛世信息技术有限公司	5
25	深圳开源互联网安全技术有限公司	5
26	杭州木链物联网科技有限公司	4
27	上海安识网络科技有限公司	4
28	成都科来软件有限公司	4
29	北京智游网安科技有限公司	4
30	个人	3

31	远江盛邦（北京）网络安全科技股份有限公司	2
32	长扬科技（北京）有限公司	2
33	清华大学	2
34	哈尔滨理工大学	2
35	北京邮电大学	2
36	北京天融信网络安全技术有限公司	2
37	知道创宇	1
38	上海三零卫士信息安全有限公司	1
39	北京威努特技术有限公司	1
40	深信服科技股份有限公司	1
41	山东潍微科技股份有限公司	1
42	锐捷网络股份有限公司	1
43	广州竞远安全技术股份有限公司	1
报送总计		7156

三、重大漏洞预警

3.1 微软多个安全漏洞的预警

近日，微软官方发布了多个安全漏洞的公告，包括 Word 远程代码执行漏洞（CNNVD-202003-544 、CVE-2020-0852）、LNK 远程代码执行漏洞（CNNVD-202003-605、CVE-2020-0684）、Microsoft SharePoint 跨站脚本漏洞（CNNVD-202003-406、CVE-2020-0891）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。

目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

本次漏洞公告涉及 Windows 操作系统、Word、SharePoint、脚本引擎、Windows 图形设备接口 (GDI)、Media Foundation、Microsoft Dynamics Business Central 等 Windows 平台下应用软件和组件。微软多个产品和系统版本受漏洞影响，具体影响范围可访问 https://portal.msrc.microsoft.com/zh-cn/security-guidance 查询，漏洞详情如下：

1、Word 远程代码执行漏洞（CNNVD-202003-544 、CVE-2020-0852）

漏洞简介：当 Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的上下文中执行操作。若要利用此漏洞，用户必须使用 Microsoft Word 软件的受影响版本打开经特殊设计的文件，才可触发此漏洞。

2、LNK 远程代码执行漏洞（CNNVD-202003-605、CVE-2020-0684）

漏洞简介：如果用户在 Windows 中处理了.LNK 文件，则 Microsoft Windows 会触发一个远程代码执行漏洞，攻击者可远程执行代码。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。与拥有管理用户权限的用户相比，帐户权限较小的用户受到的影响更小。

3、Microsoft SharePoint 跨站脚本漏洞（CNNVD-202003-406、CVE-2020-0891）

漏洞简介：当受影响的 SharePoint 服务器无法正确清理经特殊设计的请求时，存在此漏洞。经过身份验证的攻击者可能会向受影响的 SharePoint Server 发送经特殊设计请求，从而利用此漏洞。成功利用此漏洞的攻击者可能会在受影响的系统上执行跨站脚本攻击，并在当前用户的上下文中运行脚本。借助这些攻击，攻击者可以读取无权读取的内容，并更改权限、删除内容、窃取敏感信息（如浏览器 Cookie）以及在受害者的浏览器中注入恶意内容。

4、脚本引擎内存损坏漏洞（CNNVD-202003-590、CVE-2020-0768）

漏洞简介：在 Microsoft 浏览器脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

5、GDI+远程代码执行漏洞（CNNVD-202003-422、CVE-2020-0881）

漏洞简介：Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

6、Media Foundation 内存损坏漏洞（CNNVD-202003-469、CVE-2020-0801）

漏洞简介：当 Windows Media Foundation 不正确地处理内存中对象时，会触发内存损坏漏洞。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。攻击者可能通过多种方式利用此漏洞，包括诱使用户打开经特殊设计的文档或诱使用户访问恶意网页。

7、Microsoft Dynamics Business Central 远程代码执行漏洞（CNNVD-202003-510、CVE-2020-0905）

漏洞简介：Microsoft Dynamics Business Central 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者的服务器上执行任意命令。要利用此漏洞，经身份验证的攻击者需要诱使受害者连接到恶意的 Dynamics Business Central 客户端。

修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方链接地址如下：

序号	漏洞名称	官方链接
1	Word 远程代码执行漏洞（CNNVD-202003-544、CVE-2020-0852）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0852
2	LNK 远程代码执行漏洞（CNNVD-202003-605、CVE-2020-0684）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0684
3	Microsoft SharePoint 跨站脚本漏洞（CNNVD-202003-406、CVE-2020-0891）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0891
4	脚本引擎内存损坏漏洞（CNNVD-202003-590、	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0768

	CVE-2020-0768）	
5	GDI+远程代码执行漏洞（CNNVD-202003-422、CVE-2020-0881）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0881
6	Media Foundation 内存破坏漏洞（CNNVD-202003-469、CVE-2020-0801）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0801
7	Microsoft Dynamics Business Central 远程代码执行漏洞（CNNVD-202003-510、CVE-2020-0905）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0905