信息安全漏洞通报

2020 年 1 月国家信息安全漏洞库（CNNVD）

本 期 导 读

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2020 年 1 月份采集安全漏洞共 1321 个。

本月接报漏洞 2757 个，其中信息技术产品漏洞（通用型漏洞）58 个，网络信息系统漏洞（事件型漏洞）2699 个。

重大漏洞预警

1、微软多个安全漏洞：包括 Windows RDP 网关服务器远程代码执行漏洞（CNNVD-202001-475、CVE-2020-0610）、Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202001-503、CVE-2020-0611）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。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。

2、Oracle Weblogic T3 协议安全漏洞(CNNVD-202001-667、CVE-2020-2546)和 Oracle Weblogic WLS 组件 IIOP 协议安全漏洞(CNNVD-202001-675、CVE-2020-2551)：攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行，最终控制 WebLogic 服务器。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 1 月份新增安全漏洞共 1321 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 205 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 14.61%。本月新增漏洞中，超危漏洞 136 个、高危漏洞 477 个、中危漏洞 660 个、低危漏洞 48 个，相应修复率分别为 69.85%、74.84%、77.72%以及 85.41%。合计 1006 个漏洞已有修复补丁发布，本月整体修复率 76.15%。

截至 2020 年 1 月 31 日，CNNVD 采集漏洞总量已达 139143 个。

1.1 漏洞增长概况

2020 年 1 月新增安全漏洞 1321 个，与上月（1478 个）相比减少了 10.62%。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 1602 个。

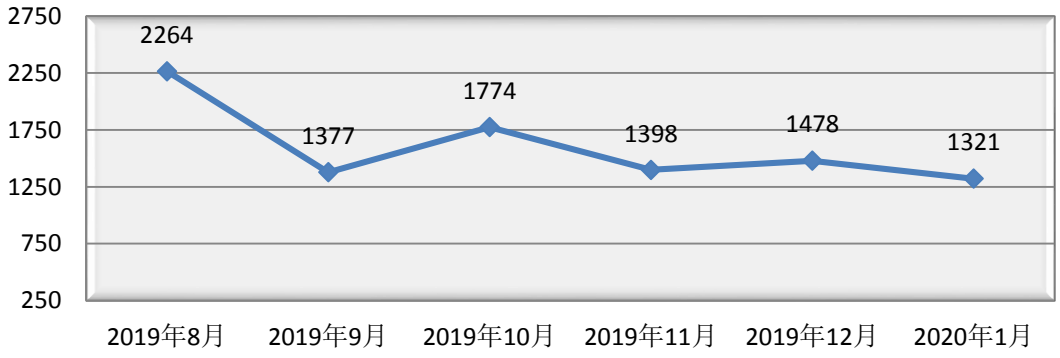

图 1 2019 年 8 月至 2020 年 1 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

1月厂商漏洞数量分布情况如表1所示，Oracle公司漏洞达到205个，占本月漏洞总量的 15.52%。本月微软公司的漏洞数量均有所上升，谷歌、IBM等厂商的漏洞数量出现较不同程度的下降。

表1　2020年1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	205	15.52%
2	微软	50	3.79%
3	思科	44	3.33%
4	GitLab	36	2.73%
5	Qualcomm	29	2.20%
6	IBM	20	1.51%
7	RedHat	19	1.44%
8	谷歌	18	1.36%
9	华为	17	1.29%
10	Mozilla	15	1.14%

1.2.2 漏洞产品分布

1 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36条，其中桌面操作系统30条，服务器操作系统35条。本月Windows 10漏洞数量最多，共32个，占主流操作系统漏洞总量的17.20%，排名第一。

表2　2020年1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	32
2	Windows Server 2016	31

3	Windows Server 2012	26
4	Windows 8.1	23
5	Windows Rt 8.1	22
6	Windows Server 2008	19
7	Windows 7	18
8	Android	13
9	Linux Kernel	2

*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

1 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 14.61%。

表 32020 年 1 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	193	14.61%
2	缓冲区错误	92	6.96%
3	信息泄露	74	5.60%
4	输入验证错误	69	5.22%
5	资源管理错误	54	4.09%
6	代码问题	50	3.79%
7	操作系统命令注入	37	2.80%
8	授权问题	34	2.57%
9	跨站请求伪造	32	2.42%
10	SQL 注入	31	2.35%
11	路径遍历	31	2.35%

12	信任管理问题	22	1.67%
13	访问控制错误	20	1.51%
14	注入	9	0.68%
15	后置链接	7	0.53%
16	环境问题	7	0.53%
17	加密问题	5	0.38%
18	命令注入	4	0.30%
19	竞争条件问题	4	0.30%
20	权限许可和访问控制问题	4	0.30%
21	代码注入	3	0.23%
22	日志信息泄露	2	0.15%
23	安全特征问题	2	0.15%
24	数据伪造问题	2	0.15%
25	数字错误	1	0.08%
26	安全特征问题	1	0.07%

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。1 月漏洞危害等级分布如图 2 所示，其中超危漏洞 136 条，占本月漏洞总数的 10.30%。

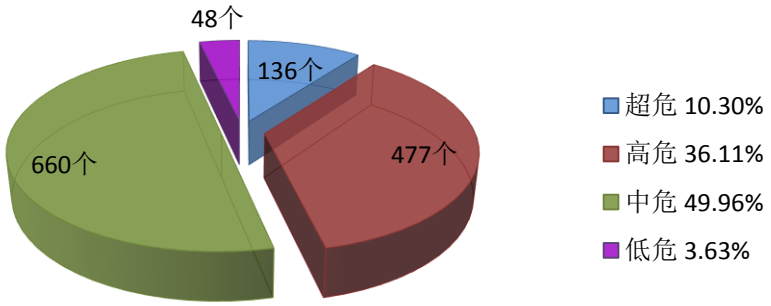

图 2　2020 年 1 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

1 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 85.41%，超危漏洞修复率最低，比例为 69.85%。与上月相比，本月超、高危漏洞修复率都有所上升。总体来看，本月整体修复率上升，由上月的 59.95%上升至本月的 76.15%。

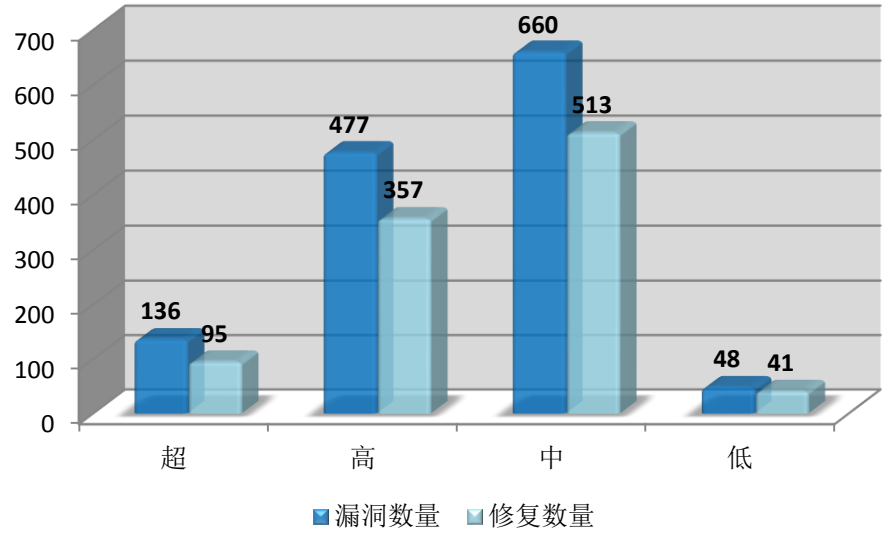

图 3　2020 年 1 月漏洞修复数量统计

1.3.2　厂商修复情况

1 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、Mozilla、Google 等十个厂商共 453 条漏洞，占本月漏洞总数的 34.06%，漏洞修复率为 94.48%，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、Mozilla、Google、华为、Qualcomm、GitLab 等公司本月漏洞修复率均为 100%，共 428 条漏洞已全部修复。

表 4　2020 年 1 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	205	205	100.00%
2	Microsoft	50	49	98.00%
3	Cisco	44	41	93.18%
4	GitLab	36	36	100.00%
5	Qualcomm	29	29	100.00%
6	IBM	20	18	90.00%
7	RedHat	19	0	0.00%
8	Google	18	18	100.00%
9	华为	17	17	100.00%
10	Mozilla	15	15	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 136 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 1 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	信任管理问题	CNNVD-202001-041	Cisco	Cisco Data Center Network Manager 信任管理问题漏洞
		CNNVD-202001-047	Cisco	
		CNNVD-202001-1371	HashiCorp	
2	资源管理错误	CNNVD-202001-1011	WebKitGTK	Google Chromium speech recognizer 组件资源管理错误漏洞
		CNNVD-202001-867	Google	
3	输入验证错误	CNNVD-202001-1014	Ruckus Wireless	Microsoft .NET Framework 输入验证错误漏洞
		CNNVD-202001-475	Microsoft	
		CNNVD-202001-486	Microsoft	
		CNNVD-202001-510	Microsoft	

		CNNVD-202001-114	LiteSpeedTechnologie	
		CNNVD-202001-1094	GNU	
		CNNVD-202001-017	Docker	
		CNNVD-202001-1122	Cisco	
4	授权问题	CNNVD-202001-1077	CTFd	DTEN D5 和 DTEN D7 授权问题漏洞
		CNNVD-202001-1319	netgear	
		CNNVD-202001-1320	netgear	
		CNNVD-202001-1223	GitLab	
		CNNVD-202001-126	DTEN	
		CNNVD-202001-1356	Apereo	
5	缓冲区错误	CNNVD-202001-949	AMD	Adobe Illustrator CC 安全漏洞
		CNNVD-202001-957	AMD	
		CNNVD-202001-529	Adobe	
		CNNVD-202001-535	Adobe	
		CNNVD-202001-537	Adobe	
		CNNVD-202001-538	Adobe	
6	代码问题	CNNVD-202001-054	FasterXML	FasterXML Jackson jackson-databind 代码问题漏洞
		CNNVD-202001-1374	Simplejobscript	
		CNNVD-202001-1329	OSSEC	
		CNNVD-202001-1311	magento	
		CNNVD-202001-962	Honeywell	
		CNNVD-202001-1228	gitlab	
7	SQL 注入	CNNVD-202001-1090	Koha	IBM Jazz Reporting Service SQL 注入漏洞
		CNNVD-202001-1093	Koha	
		CNNVD-202001-325	IBM	
		CNNVD-202001-958	Honeywell	
		CNNVD-202001-1349	exlibrisgroup	

1. Cisco Data Center Network Manager 信任管理问题漏洞（CNNVD-202001-047）

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

Cisco DCNM 11.3 之前版本中的身份验证机制存在信任管理问题

漏洞。远程攻击者可借助静态密钥创建有效的会话令牌利用该漏洞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-20200102-dcnm-auth-bypass

2. Google Chromium speech recognizer 组件资源管理错误漏洞（CNNVD-202001-867）

Google Chromium 是美国谷歌（Google）的一款开源的 Web 浏览器。speech recognizer 是其中的一个语音识别组件。

Google Chromium 79.0.3945.130 之前版本中的 speech recognizer 组件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。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/01/stable-channel-update-for-desktop_16.html

3. Microsoft .NET Framework 输入验证错误漏洞（CNNVD-202001-510）

Microsoft .NET Framework 是美国微软（Microsoft）公司的一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。该平台包括 C#和 Visual Basic 编程语言、公共语言运行库和广泛的类库。

Microsoft .NET Framework 中存在远程代码执行漏洞，该漏洞源

于程序无法正确验证输入。攻击者可通过提交输入利用该漏洞控制受影响的系统。以下产品及版本受到影响：Microsoft .NET Framework 3.0 SP2 版本，3.5 版本，3.5.1 版本，4.5.2 版本，4.6 版本，4.6.1 版本，4.6.2 版本，4.7 版本，4.7.1 版本，4.7.2 版本，4.8 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646

4. DTEN D5 和 DTEN D7 授权问题漏洞（CNNVD-202001-126）

DTEN D5 和 DTEN D7 都是 DTEN 公司的一款触控笔。

DTEN D5 和 D7 1.3.4 之前版本中存在安全漏洞。攻击者可利用该漏洞进行系统管理并执行任意代码，获取 Zoom Client 所显示的数据。

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.displayten.com.cn/

5. Adobe Illustrator CC 安全漏洞（CNNVD-202001-529）

Adobe Illustrator CC 是一种应用于出版、多媒体和在线图像的工业标准矢量插画的软件。

基于 Windows 平台的 Adobe Illustrator CC 24.0 及之前版本中存在内存损坏漏洞。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。

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/illustrator/apsb20-03.html

6. FasterXML Jackson jackson-databind 代码问题漏洞（CNNVD-202001-054）

FasterXML Jackson 是美国 FasterXML 公司的一款适用于 Java 的数据处理工具。jackson-databind 是其中的一个具有数据绑定功能的组件。

FasterXMLjackson-databind 2.9.10.2 之前的 2.x 版本中存在代码问题漏洞。该漏洞源于网络系统或产品的代码开发过程中存在设计或实现不当的问题。

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/FasterXML/jackson-databind/commit/fc4214a883dc087070f25da738ef0d49c2f3387e

7. IBM Jazz Reporting Service SQL 注入漏洞（CNNVD-202001-325）

IBM Jazz Reporting Service（JRS）是美国 IBM 公司的一套即用型报告组件。该产品包括报表生成、数据收集和生命周期查询等功能。。

IBM JRS 6.0.6.1 版本中存在 SQL 注入漏洞。远程攻击者可借助特制的 SQL 语句利用该漏洞查看，添加，修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://github.com/FasterXML/jackson-databind/commit/fc4214a883dc087070f25da738ef0d49c2f3387e

1.4.2 高危漏洞实例

本月高危漏洞共 477 个，其中重点漏洞实例如表 6 所示。

表 62020 年 1 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	信息泄露	CNNVD-202001-005	友讯	Adobe Experience Manager 信息泄露漏洞
		CNNVD-202001-1007	Vanilla Forums	
		CNNVD-202001-1336	JetBrains	
		CNNVD-202001-1369	JetBrains	
		CNNVD-202001-1057	HashiCorp	
		CNNVD-202001-098	GitLab	
		CNNVD-202001-1222	GitLab	
		CNNVD-202001-1230	GitLab	
		CNNVD-202001-1250	Apache	
		CNNVD-202001-626	Adobe	
		CNNVD-202001-628	Adobe	
2	信任管理问题	CNNVD-202001-019	SuperMicro	Cisco Data Center Network Manager 信任管理问题漏洞
		CNNVD-202001-1353	Opencast	
		CNNVD-202001-468	Microsoft	
		CNNVD-202001-1335	JetBrains	
		CNNVD-202001-1069	IXP Data	
		CNNVD-202001-930	fujixerox	
		CNNVD-202001-935	fujixerox	
		CNNVD-202001-040	Cisco	
		CNNVD-202001-1240	Android	
3	输入验证错误	CNNVD-202001-1003	UseBB	多款 Qualcomm 产品输入验证错误漏洞
		CNNVD-202001-1352	Trend Micro	
		CNNVD-202001-170	Qualcomm	
		CNNVD-202001-178	Qualcomm	
		CNNVD-202001-180	Qualcomm	
		CNNVD-202001-181	Qualcomm	
		CNNVD-202001-182	Qualcomm	
		CNNVD-202001-203	Qualcomm	
		CNNVD-202001-053	Pillow	
		CNNVD-202001-1346	OAuth2 Proxy	
		CNNVD-202001-220	Mozilla	
		CNNVD-202001-469	Microsoft	
		CNNVD-202001-474	Microsoft	
		CNNVD-202001-503	Microsoft	

		CNNVD-202001-1150	Lustre	
		CNNVD-202001-003	libsixel	
		CNNVD-202001-1066	IXP Data	
		CNNVD-202001-1261	IBM	
		CNNVD-202001-120	Haxx	
		CNNVD-202001-937	grin	
		CNNVD-202001-093	GitLab	
		CNNVD-202001-539	GE	
		CNNVD-202001-1345	Cisco	
4	授权问题	CNNVD-202001-884	华为	Schneider Electric EcoStruxure Geo SCADA Expert 授权问题漏洞
		CNNVD-202001-138	Schneider Electric	
		CNNVD-202001-140	Schneider Electric	
		CNNVD-202001-394	RICOH	
		CNNVD-202001-406	RICOH	
		CNNVD-202001-205	Jamf	
		CNNVD-202001-608	CloudBees	
5	路径遍历	CNNVD-202001-1016	troglobit	Cisco Data Center Network Manager 路径遍历漏洞
		CNNVD-202001-1013	Ruckus Wireless	
		CNNVD-202001-1247	Polycom	
		CNNVD-202001-1091	Koha	
		CNNVD-202001-1092	Koha	
		CNNVD-202001-1063	IXP Data	
		CNNVD-202001-918	DIMO	
		CNNVD-202001-030	Cisco	
		CNNVD-202001-031	Cisco	
		CNNVD-202001-032	Cisco	
		CNNVD-202001-1163	AlienVault	
6	跨站请求伪造	CNNVD-202001-1277	WordPress	OSIsoft PI Vision 跨站请求伪造漏洞
		CNNVD-202001-1293	Webargs	
		CNNVD-202001-1006	UseBB	
		CNNVD-202001-393	RICOH	
		CNNVD-202001-839	Pivotal Software	
		CNNVD-202001-521	OSIsoft	
		CNNVD-202001-301	Juniper Networks	
		CNNVD-202001-940	Facebook	
		CNNVD-202001-597	CloudBees	
		CNNVD-202001-611	CloudBees	
		CNNVD-202001-242	Cisco	

		CNNVD-202001-1276	ASUS	
		CNNVD-202001-999	AEF	
		CNNVD-202001-1134	Adive	
7	缓冲区错误	CNNVD-202001-051	Pillow	Microsoft Internet Explorer 缓冲区错误漏洞
		CNNVD-202001-052	Pillow	
		CNNVD-202001-055	Pillow	
		CNNVD-202001-1252	NetHack	
		CNNVD-202001-1253	NetHack	
		CNNVD-202001-1254	NetHack	
		CNNVD-202001-470	Microsoft	
		CNNVD-202001-504	Microsoft	
		CNNVD-202001-513	Microsoft	
		CNNVD-202001-1324	OSSEC	
		CNNVD-202001-1325	OSSEC	
		CNNVD-202001-048	OpenCV	
8	SQL 注入	CNNVD-202001-034	Cisco	Cisco Data Center Network Manager SQL 注入漏洞
		CNNVD-202001-038	Cisco	
		CNNVD-202001-1071	Plone	
		CNNVD-202001-1314	magento	
		CNNVD-202001-1290	contao	
9	其它	CNNVD-202001-876	Microsoft	Microsoft Internet Explorer 安全漏洞

1. Adobe Experience Manager 信息泄露漏洞(CNNVD-202001-626）

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。

Adobe AEM 6.5版本、6.4版本和6.3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。

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/experience-manager/apsb20-01.html

2. Cisco Data Center Network Manager 信任管理问题漏洞

(CNNVD-202001-040）

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

Cisco DCNM 11.3(1)之前版本中的 Web 管理界面存在信任管理问题漏洞。远程攻击者可借助静态凭证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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-auth-bypass

3. 多款 Qualcomm 产品输入验证错误漏洞(CNNVD-202001-178）

Qualcomm MDM9607 等都是美国高通（Qualcomm）公司的产品。MDM9607 是一款中央处理器（CPU）产品。SDM660 是一款中央处理器（CPU）产品。SDX55 是一款调制解调器。

多款 Qualcomm 产品中的 Audio 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。以下产品及版本受到影响：Qualcomm MDM9607；Nicobar；Rennell；SA6155P；SDM660；SDX55；SM6150；SM7150；SM8150；SM8250；SXR2130。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.qualcomm.com/company/product-security/bulletins/january-2020-bulletin

4. Schneider Electric EcoStruxure Geo SCADA Expert 授权问题漏

洞(CNNVD-202001-138）

Schneider Electric EcoStruxure Geo SCADA Expert（ClearSCADA）是法国施耐德电气（Schneider Electric）公司的一套数据采集和监控软件（SCADA）。

Schneider Electric EcoStruxure Geo SCADA Expert (ClearSCADA)中存在授权问题漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。以下产品及版本受到影响：ClearSCADA 2017 R3 版本，ClearSCADA 2017 R2 版本，ClearSCADA 2017 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.se.com/ww/en/download/document/SEVD-2019-344-05

5. Cisco Data Center Network Manager 路径遍历漏洞

(CNNVD-202001-030）

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

Cisco DCNM 11.3(1)之前版本中的 Application Framework 功能存在路径遍历漏洞，该漏洞源于程序没有充分验证发送到 Application Framework 端点的用户输入。远程攻击者可通过发送特制的请求利用该漏洞以管理权限在系统中读取，编写或执行任意文件。

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-20200102-dcnm-path-trav

6. OSIsoft PI Vision 跨站请求伪造漏洞(CNNVD-202001-521）

OSIsoft PI Vision 是美国 OSIsoft 公司的一套支持从移动设备访问 PI System 数据的可视化工具，它支持自配置趋势、图像、数据值等以呈现数据信息。

OSIsoft PI Vision 2019 之前版本中存在跨站请求伪造漏洞。该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。。

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.osisoft.cn/

7. Microsoft Internet Explorer 缓冲区错误漏洞

(CNNVD-202001-504）

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 9、10 和 11 中存在远程代码执行漏洞，该漏洞源于程序没有正确访问内存对象。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/en-US/security-guidance/advisory/CVE-2020-0640

8. Cisco Data Center Network Manager SQL 注入漏洞

(CNNVD-202001-034）

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

Cisco DCNM 11.3(1)之前版本中的 SOAP API 存在 SQL 注入漏洞，该漏洞源于程序没有充分验证提交到该 API 的用户输入。远程攻击者可通过发送特制的请求利用该漏洞执行任意的 SQL 命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-sql-inject

9. Microsoft Internet Explorer 安全漏洞漏洞(CNNVD-202001-876）

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 9、10 和 11 中脚本引擎处理内存对象的方法存在安全漏洞。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。

目前厂商已发布公告，缓解漏洞带来的危害，公告链接：

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200001

二、接报漏洞情况

本月接报漏洞 2757 个，其中信息技术产品漏洞（通用型漏洞）

58 个，网络信息系统漏洞（事件型漏洞）2699 个。

表 7 2020 年 1 月漏洞接报情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	1243
2	网神信息技术（北京）股份有限公司	858
3	内蒙古洞明科技有限公司	271
4	内蒙古奥创科技有限公司	81
5	山东新潮信息技术有限公司	59
6	北京华云安信息技术有限公司	52
7	太极计算机股份有限公司	49
8	广州锦行网络科技有限公司	21
9	北京华云安信息技术有限公司	17
10	国发中新（北京）科技发展有限公司	15
11	上海安洵信息技术有限公司	13
12	北京启明星辰信息安全技术有限公司	11
13	广州市昊恒信息科技有限公司	10
14	广西电网有限责任公司电力科学研究院	8
15	北京圣博润高新技术股份有限公司	8
16	上海三零卫士信息安全有限公司	8
17	上海安识网络科技有限公司	6
18	个人	3
19	北京智游网安科技有限公司	3
20	中国电信集团系统集成有限责任公司	3

21	众安天下	2
22	广州万方计算机科技有限公司	2
23	西安交大捷普网络科技有限公司	2
24	天津市兴先道科技有限公司	2
25	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	2
26	深圳开源互联网安全技术有限公司	1
27	山东正中信息技术股份有限公司——信息安全部	1
28	亚信科技（成都）有限公司	1
29	河南听潮盛世信息技术有限公司	1
30	北京威努特技术有限公司	1
31	北京神州绿盟科技有限公司工业物联网安全实验室	1
32	西安电子科技大学、中国电子技术标准化研究院	1
33	哈尔滨安天科技股份有限公司	1
报送总计		2757

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 Windows CryptoAPI 欺骗漏洞（CNNVD-202001-468、CVE-2020-0601）、Windows RDP 网关服务器远程代码执行漏洞（CNNVD-202001-475、CVE-2020-0610）、Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202001-503、CVE-2020-0611）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 系统、CryptoAPI 、RDP 网关、Internet Explorer、Microsoft Excel、.NET Framework、ASP.NET Core、Windows Search 索引器等 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、Windows CryptoAPI 欺骗漏洞（CNNVD-202001-468、CVE-2020-0601）

漏洞简介：在 Windows CryptoAPI（Curt32.dll）验证 Elliptic Curve Cryptography (ECC)证书的方式中存在欺骗漏洞。攻击者可以通过使用欺骗性的代码签名证书对恶意可执行文件进行签名来利用此漏洞，从而使该文件看似来自受信任的合法来源。用户将无法知道该文件是恶意文件，因为数字签名看似来自受信任的程序提供。成功利用漏洞的攻击者可以进行中间人攻击，并对相关用户与受影响软件的机密信息进行解密。

2、Windows RDP 网关服务器远程代码执行漏洞（CNNVD-202001-475、CVE-2020-0610）（CNNVD-202001-486、CVE-2020-0609）

漏洞简介：当未经身份验证的攻击者使用 RDP 连接到目标系统并发送经特殊设计的请求时，Windows 远程桌面协议 (RDP) 网关服务器会触发远程代码执行漏洞。此漏洞是预身份验证，无需用户交互。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。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。

3、Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202001-503、CVE-2020-0611）

漏洞简介： Windows 远程桌面客户端中存在一个远程代码执行漏洞，当用户连接到恶意服务器时，会触发该漏洞。成功利用此漏洞的攻击者可以在连接客户端的计算机中执行任意代码，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。

4、Internet Explorer 内存损坏漏洞（CNNVD-202001-504、CVE-2020-0640）

漏洞简介：当 Internet Explorer 不正确地访问内存中的对象时，会触发一个远程代码执行漏洞。该漏洞可以使攻击者在当前用户的上下文中执行任意代码，以此来破坏内存。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，如果当前用户使用管理用户权限登录，那么攻击者便可控制受影响的系统。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。

5、Microsoft Excel 远程代码执行漏洞（CNNVD-202001-513、CVE-2020-0650）（CNNVD-202001-514、CVE-2020-0651）（CNNVD-202001-520、CVE-2020-0653）

漏洞简介：当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，那么攻击者就可以控制受影响的系统。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、.NET Framework 远程代码执行漏洞（CNNVD-202001-510、CVE-2020-0646）（CNNVD-202001-474、CVE-2020-0605）（CNNVD-202001-469、CVE-2020-0606）

漏洞简介：当 Microsoft .NET Framework 未能正确验证输入时，会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影

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。

7、ASP.NET Core 远程代码执行漏洞（CNNVD-202001-470、CVE-2020-0603）

漏洞简介：当 ASP.NET Core 软件无法处理内存中的对象时，会触发一个远程代码执行漏洞。成功利用该漏洞的攻击者会在当前用户的上下文中运行任意代码，如果当前用户使用管理用户权限登录，那么攻击者就可以控制受影响的系统。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。

8、Windows Search 索引器特权提升漏洞（CNNVD-202001-485、CVE-2020-0625）

漏洞简介：Windows Search 索引器处理内存中对象的方式中存在特权提升漏洞。成功利用此漏洞的攻击者可能会利用提升的特权执行代码。若要利用此漏洞，攻击者需要在本地经过身份验证，并运行经特殊设计的应用程序。

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	Windows CryptoAPI 欺骗漏洞（CNNVD-202001-468、CVE-2020-0601）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0601

2	Windows RDP 网关服务器远程代码执行漏洞（CNNVD-202001-475、CVE-2020-0610）（CNNVD-202001-486、CVE-2020-0609）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0610 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0609
3	Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202001-503、CVE-2020-0611）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0611
4	Internet Explorer 内存损坏漏洞（CNNVD-202001-504、CVE-2020-0640）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0640
5	Microsoft Excel 远程代码执行漏洞（CNNVD-202001-513、CVE-2020-0650）（CNNVD-202001-514、CVE-2020-0651）（CNNVD-202001-520、CVE-2020-0653）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0650 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0651 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0653
6	.NET Framework 远程代码执行漏洞（CNNVD-202001-510、CVE-2020-0646）（CNNVD-202001-474、CVE-2020-0605）（CNNVD-202001-469、CVE-2020-0606）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0646 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0605 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0606
7	ASP.NET Core 远程代码执行	https://portal.msrc.microsoft.com/zh-CN/security-gui

	漏洞（CNNVD-202001-470、CVE-2020-0603）	dance/advisory/CVE-2020-0603
8	Windows Search 索引器特权提升漏洞（CNNVD-202001-485、CVE-2020-0625）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0

3.2Oracle WebLogic 多个安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Oracle Weblogic T3 协议安全漏洞(CNNVD-202001-667、CVE-2020-2546)和 Oracle Weblogic WLS 组件 IIOP 协议安全漏洞(CNNVD-202001-675、CVE-2020-2551)情况的报送。攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行，最终控制 WebLogic 服务器。Oracle WebLogic Server 10.3.6.0、12.1.3.0、12.2.1.3、12.2.1.4 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

OracleWebLogicServer 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。T3 协议是用于在 WebLogic 服务器和其他类型的

Java 程序之间传输信息的协议。IIOP 协议是一个用于 CORBA 2.0 及兼容平台，用来在 CORBA 对象请求代理之间交流的协议。

1、Oracle WebLogic T3 协议安全漏洞(CNNVD-202001-667、CVE-2020-2546)

攻击者可以通过 T3 协议对存在漏洞的 WebLogicServer 进行反序列化攻击，成功利用该漏洞的攻击者可以对目标系统实现远程代码执行，进而控制 WebLogic 服务器。

2、Oracle WebLogic WLS 组件 IIOP 协议安全漏洞(CNNVD-202001-675、CVE-2020-2551)

攻击者可以在未授权的情况下通过 IIOP 协议对存在漏洞的 Web Logic Server 组件进行反序列化攻击，成功利用该漏洞的攻击者可以对目标系统实现远程代码执行，进而控制 WebLogic 服务器。

危害影响

1、Oracle WebLogic T3 协议安全漏洞(CNNVD-202001-667、CVE-2020-2546)

成功利用该漏洞的攻击者可以对目标系统实现远程代码执行，进而控制 WebLogic 服务器。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

2、Oracle WebLogic WLS 组件 IIOP 协议安全漏洞(CNNVD-202001-675、CVE-2020-2551)

成功利用该漏洞的攻击者可以对目标系统实现远程代码执行，进而控制 WebLogic 服务器。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
Oracle WebLogic Server 12.2.1.4

安全建议

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/security-alerts/cpujan2020.html