信息安全漏洞通报

2020 年 2 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 2 月份采集安全漏洞共 1246 个。

本月接报漏洞 1230 个，其中信息技术产品漏洞（通用型漏洞）83 个，网络信息系统漏洞（事件型漏洞）1147 个。

重大漏洞预警

1、思科 CDP 设备多个安全漏洞：包括思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、CVE-2020-3111）等多个漏洞。成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。思科 Firepower 1000 Series、IOS XRv 9000 Router、Nexus 1000V Switch、IP Conference Phone 7832、Video Surveillance 8000 Series IP Camera 等多款设备均受此漏洞影响。目前，思科官方已发布漏洞补丁修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

2、微软多个安全漏洞：包括 Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）、Windows LNK 远程执行代

码漏洞（CNNVD-202002-544、CVE-2020-0729）、Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）；Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681 ； CNNVD-202002-538 、 CVE-2020-0734 ； CNNVD-202002-646、CVE-2020-0817）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。

3、Apache Tomcat 文件包含漏洞（CNNVD-202002-1052、CVE-2020-1938）：成功利用漏洞的攻击者可以读取 Tomcat 所有 webapp 目录下的任意文件。该漏洞影响包括 Apache Tomcat 9.x、Apache Tomcat 8.x、Apache Tomcat 7.x 、Apache Tomcat 6.x 等多个版本的 Tomcat。目前，Apache 官方已发布公告对修复该漏洞做出说明，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 2 月份新增安全漏洞共 1246 个，从厂商分布来看，Microsoft 公司产品的漏洞数量最多，共发布 102 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 12.04%。本月新增漏洞中，超危漏洞 179 个、高危漏洞 473 个、中危漏洞 571 个、低危漏洞 23 个，相应修复率分别为 73.18%、81.40%、69.70%以及 82.61%。合计 933 个漏洞已有修复补丁发布，本月整体修复率 74.88%。

截至 2020 年 2 月 29 日，CNNVD 采集漏洞总量已达 140468 个。

1.1 漏洞增长概况

2020 年 2 月新增安全漏洞 1246 个，与上月（1321 个）相比减少了 5.70%。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 1432 个。

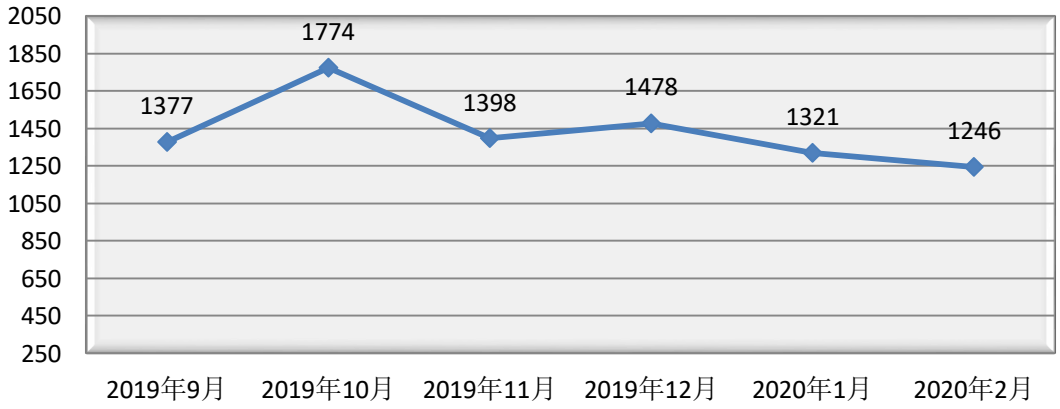

图 1 2019 年 9 月至 2020 年 2 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2 月厂商漏洞数量分布情况如表 1 所示，Microsoft 公司漏洞达到 102 个，占本月漏洞总量的 8.19%。本月 Microsoft、Google 等厂商的漏洞数量均有所上升，Cisco、Oracle 等厂商的漏洞数量出现较不同程度的下降。

表 1　2020 年 2 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	Microsoft	102	8.19%
2	Google	57	4.57%
3	IBM	53	4.25%
4	Adobe	44	3.53%
5	Cisco	41	3.29%
6	Moxa	37	2.97%
7	CloudBees	26	2.09%
8	华为	25	2.01%
9	Nextcloud	21	1.69%
10	Linux 基金会	20	1.61%

1.2.2 漏洞产品分布

2 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 84 条，其中桌面操作系统 83 条，服务器操作系统 81 条。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 13.77%，排名第一。

表 2　2020 年 2 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 1903	75
3	Windows Server 1803	73
4	Windows Server 2016	66
5	Windows Server 2012	53
6	Windows 7	51
7	Windows 8.1	50
8	Windows Rt 8.1	50
9	Windows Server 2008	49
10	Android	15
11	Linux Kernel	10
12	Apple macOS	1

*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

2 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 12.04%。

表 3 2020 年 2 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区错误	150	12.04%
2	跨站脚本	144	11.56%
3	输入验证错误	106	8.51%
4	信息泄露	84	6.74%
5	资源管理错误	64	5.14%
6	代码问题	59	4.74%
7	授权问题	49	3.93%

8	跨站请求伪造	48	3.85%
9	操作系统命令注入	38	3.05%
10	注入	36	2.89%
11	SQL 注入	34	2.73%
12	路径遍历	25	2.01%
13	信任管理问题	19	1.52%
14	访问控制错误	14	1.12%
15	加密问题	7	0.56%
16	数据伪造问题	7	0.56%
17	命令注入	4	0.32%
18	竞争条件问题	4	0.32%
19	代码注入	4	0.32%
20	后置链接	2	0.16%
21	环境问题	2	0.16%
22	格式化字符串错误	2	0.16%
23	安全特征问题	2	0.16%
24	权限许可和访问控制问题	2	0.16%
25	数字错误	1	0.08%
26	日志信息泄露	1	0.08%

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。2 月漏洞危害等级分布如图 2 所示，其中超危漏洞 179 条，占本月漏洞总数的 14.37%。

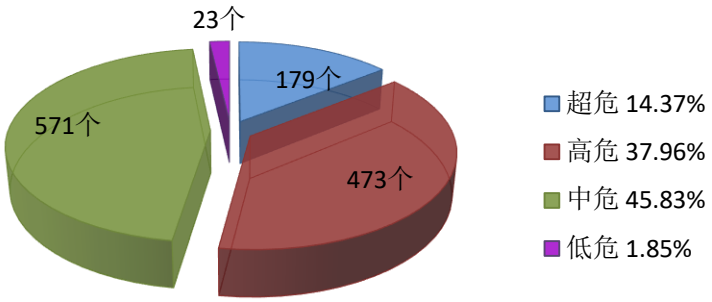

图 2　2020 年 2 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

2 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 82.61%，中危漏洞修复率最低，比例为 69.70%。与上月相比，本月中、低危漏洞修复率都有所下降。总体来看，本月整体修复率下降，由上月的 76.15%下降至本月的 74.88%。

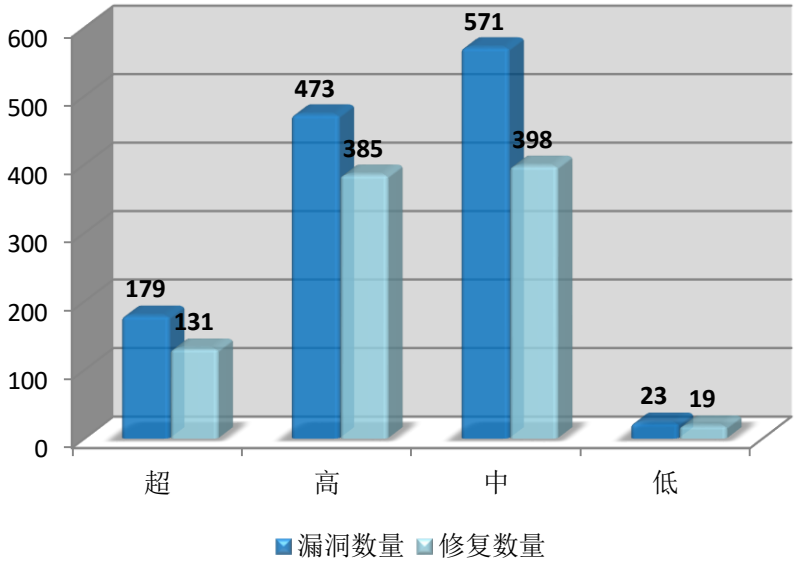

图 3　2020 年 2 月漏洞修复数量统计

1.3.2 厂商修复情况

2 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 426 条漏洞，占本月漏洞总数的 34.19%，漏洞修复率为 92.25%，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 Adobe 、华为 、Nextcloud 等公司本月漏洞修复率均为 100%，共 382 条漏洞已全部修复。

表 4　2020 年 2 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	Microsoft	102	100	98.04%
2	Google	57	55	96.49%
3	IBM	53	52	98.11%
4	Adobe	44	44	100.00%
5	Cisco	41	39	95.12%
6	Moxa	37	36	97.30%
7	CloudBees	26	15	57.69%
8	华为	25	25	100.00%
9	Nextcloud	21	21	100.00%
10	Linux 基金会	20	6	30.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 179 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 2 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-202002-628	Adobe	Adobe Acrobat 和

		CNNVD-202002-629		Reader 资源管理错误漏洞（CNNVD-202002-628）
		CNNVD-202002-630		
		CNNVD-202002-633		
		CNNVD-202002-634		
		CNNVD-202002-635		
2	注入	CNNVD-202002-088	Dnt	IBM Spectrum Protect Plus 注入漏洞（CNNVD-202002-1078）
		CNNVD-202002-093		
		CNNVD-202002-643	Adobe	
		CNNVD-202002-1078	IBM	
		CNNVD-202002-1080		
		CNNVD-202002-1082		
		CNNVD-202002-1084		
		CNNVD-202002-1086		
		CNNVD-202002-1213	IBL	
3	信息泄露	CNNVD-202002-1164	Moxa	Moxa PT-7528 和 PT-7828 信息泄露漏洞（CNNVD-202002-1164）
		CNNVD-202002-1200		
4	信任管理问题	CNNVD-202002-053	IBM	Cisco Smart Software Manager On-Prem 信任管理问题漏洞（CNNVD-202002-985）
		CNNVD-202002-325	Polycom	
		CNNVD-202002-825	HCL	
		CNNVD-202002-985	Cisco	
		CNNVD-202002-1160	Moxa	
		CNNVD-202002-1171		
5	输入验证错误	CNNVD-202002-135	Coppermine	Zabbix SIA Zabbix 输入验证错误漏洞（CNNVD-202002-854）
		CNNVD-202002-145	PlaySMS	
		CNNVD-202002-201	Qualcomm	
		CNNVD-202002-227	Sphider	
		CNNVD-202002-661	CloudBees	
		CNNVD-202002-662		
		CNNVD-202002-854	Zabbix SIA	
		CNNVD-202002-978	IBM	
		CNNVD-202002-995	VMware	
		CNNVD-202002-1052	Apache 软件基金会	
6	授权问题	CNNVD-202002-028	eG Innovations	Synergy Systems & Solutions HUSKY RTU 6049-E70 授权问题漏洞（CNNVD-202002-593）
		CNNVD-202002-193	Wptimecapsule	
		CNNVD-202002-471	ATutor	
		CNNVD-202002-593	Synergy Systems & Solutions	
		CNNVD-202002-750	OpenVPN	
		CNNVD-202002-1039	Western Digital	
		CNNVD-202002-111	Auto-Maskin	

7	路径遍历	CNNVD-202002-1107	Yarnpkg	Yarn 路径遍历漏洞（CNNVD-202002-1107）
		CNNVD-202002-1149	Honeywell	
		CNNVD-202002-1188	Gurux	
8	跨站脚本	CNNVD-202002-804	Progress Software	Progress Software MOVEit Transfer 跨站脚本漏洞（CNNVD-202002-804）
9	缓冲区错误	CNNVD-202002-007	Nanopb	Emerson Electric OpenEnterprise SCADA Server 缓冲区错误漏洞（CNNVD-202002-923）
		CNNVD-202002-029	ppp	
		CNNVD-202002-205	Qualcomm	
		CNNVD-202002-208		
		CNNVD-202002-625	Adobe	
		CNNVD-202002-627		
		CNNVD-202002-636		
		CNNVD-202002-638		
		CNNVD-202002-1028		
		CNNVD-202002-1030		
		CNNVD-202002-728	WeeChat	
		CNNVD-202002-752	D-Link	
		CNNVD-202002-923	Emerson Electric	
		CNNVD-202002-1161	Moxa	
		CNNVD-202002-1162		
		CNNVD-202002-1163		
		CNNVD-202002-1174		
		CNNVD-202002-1215		
		CNNVD-202002-1169	OpenSMTPD	
10	访问控制错误	CNNVD-202002-241	Bosch	Bosch Video Streaming Gateway 访问控制错误漏洞（CNNVD-202002-241）
11	代码问题	CNNVD-202002-125	dotCMS	FasterXML jackson-databind 代码问题漏洞（CNNVD-202002-354）
		CNNVD-202002-164	Nuxeo	
		CNNVD-202002-236	Bosch	
		CNNVD-202002-354	FasterXML	
		CNNVD-202002-424	Red Hat	
		CNNVD-202002-723	Tiny	
		CNNVD-202002-725		
		CNNVD-202002-828	Jsreport	
		CNNVD-202002-933	Synacor	
12	操作系统命令	CNNVD-202002-426	Microvirt	LPAR2RRD 操作

	注入	CNNVD-202002-871	Xorux	系统命令注入漏洞（CNNVD-202002-871）
		CNNVD-202002-1134	Moxa	
		CNNVD-202002-1216	ZyXEL	
13	SQL 注入	CNNVD-202002-011	Django 基金会	Django SQL 注入漏洞（CNNVD-202002-011）
		CNNVD-202002-027	eG Innovations	
		CNNVD-202002-194	EyesOfNetwork	
		CNNVD-202002-428	Secom	
		CNNVD-202002-658	Enorth	
		CNNVD-202002-853	Sygnoos	

1. Adobe Acrobat 和 Reader 资源管理错误漏洞（CNNVD-202002-628）

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在当前用户的上下文中执行任意代码。以下产品及版本受到影响：

- 基于 Windows 的 Acrobat DC 2019.021.20061 及之前版本
- 基于 Windows 的 Acrobat Reader DC 2019.021.20061 及之前版本
- 基于 Windows 的 Acrobat 2015 2015.006.30508 及之前版本
- 基于 Windows 的 Acrobat Reader 2015 2015.006.30508 及之前版本
- 基于 Windows 的 Acrobat 2017 2017.011.30156 及之前版本
- 基于 macOS 平台的 Acrobat DC 2019.021.20061 及之前版本
- 基于 macOS 平台的 Acrobat Reader DC 2019.021.20061 及之前

版本

- 基于 macOS 平台的 Acrobat 2015 2015.006.30508 及之前版本
- 基于 macOS 平台的 Acrobat Reader 2015 2015.006.30508 及之前版本
- 基于 macOS 平台的 Acrobat Reader 2017 2017.011.30156 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/apsb20-05.html

2. IBM Spectrum Protect Plus 注入漏洞（CNNVD-202002-1078）

IBM Spectrum Protect Plus 是美国 IBM 公司的一套数据保护平台。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 Protect Plus 10.1.0 版本至 10.1.5 版本中存在注入漏洞。远程攻击者可借助特制的 HTTP 命令利用该漏洞在系统上执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/3178863

3. Moxa PT-7528 和 PT-7828 信息泄露漏洞（CNNVD-202002-1164）

Moxa PT-7528 和 PT-7828 都是中国台湾摩莎（Moxa）公司的一款机柜管理型交换机产品。

使用 4.0 及之前版本固件的 Moxa PT-7528 系列和使用 3.9 及之前版本固件的 PT-7828 系列中存在信息泄露漏洞。攻击者可利用该漏洞

未授权访问 Web 服务的敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.moxa.com/en/support/support/security-advisory/pt-7528-7828-ethernet-switches-vulnerabilities

4. **Cisco Smart Software Manager On-Prem 信任管理问题漏洞（CNNVD-202002-985）**

Cisco Smart Software Manager On-Prem 是美国思科（Cisco）公司的一款用于 Cisco 产品许可证管理的组件。

Cisco Smart Software Manager On-Prem 7-202001 之前版本中的 High Availability (HA)服务存在信任管理问题漏洞，该漏洞源于系统管理员无法控制带有默认静态密码的系统账户。远程攻击者可通过使用该账户利用该漏洞访问系统的敏感部分。

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-on-prem-static-cred-sL8rDs8

5. Zabbix SIA Zabbix 输入验证错误漏洞（CNNVD-202002-854）

Zabbix SIA Zabbix 是拉脱维亚 Zabbix SIA 公司的一套开源的监控系统。该系统支持网络监控、服务器监控、云监控和应用监控等。

Zabbix SIA Zabbix 2.0.6 版本中存在文件包含漏洞，该漏洞源于请求字符串清理不当。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://support.zabbix.com/browse/ZBX-6652

6. Synergy Systems & Solutions HUSKY RTU 6049-E70 授权问题漏洞（CNNVD-202002-593）

Synergy Systems & Solutions HUSKY RTU 6049-E70 是印度 Synergy Systems & Solutions 公司的一个远程终端单元（RTU）。

使用 5.0 及之前版本固件的 Synergy Systems & Solutions HUSKY RTU 6049-E70 中存在授权问题漏洞，该漏洞源于程序没有要求进行正确的身份验证。攻击者可利用该漏洞读取敏感信息或执行任意代码。

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.s3india.com/

7. Yarn 路径遍历漏洞（CNNVD-202002-1107）

Yarn 是一款开源的软件包安装、管理工具。

Yarn 1.21.1 及之前版本中存在路径遍历漏洞。攻击者可借助恶意的软件包利用该漏洞向文件系统的任意路径进行写入操作，可能执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/yarnpkg/yarn/pull/7831

8. Progress Software MOVEit Transfer 跨站脚本漏洞（CNNVD-202002-804）

Progress Software MOVEit Transfer 是美国 Progress Software 公司的一套文件传输软件。

Progress Software MOVEit Transfer 2019.1.4 之前的 2019.1 版本和 2019.2.1 之前的 2019.2 版本中存在跨站脚本漏洞，该漏洞源于 REST

API 端点没有充分地清理恶意输入。攻击者可利用该漏洞在用户浏览器中执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://community.ipswitch.com/s/article/MOVEit-Transfer-Security-Vulnerabilities-Feb-2020

9. Emerson Electric OpenEnterprise SCADA Server 缓冲区错误漏洞（CNNVD-202002-923）

Emerson Electric OpenEnterprise SCADA Server 是美国艾默生电气（Emerson Electric）公司的一套主要用于远程石油和天然气应用的数据采集与监控系统（SCADA）服务器。

Emerson Electric OpenEnterprise SCADA Server 3.1 至 3.3.3 版本和 2.83 版本（安装并使用 Modbus 或 ROC 界面）中存在缓冲区错误漏洞。攻击者可借助特制的脚本利用该漏洞在 OpenEnterprise Server 上执行代码。

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.emerson.com/

10. Bosch Video Streaming Gateway 访问控制错误漏洞（CNNVD-202002-241）

Bosch DIVAR IP 2000 和 Bosch DIVAR IP 3000 都是德国 Bosch 公司的产品。Bosch DIVAR IP 2000 是一款 2000 系列视频录像机。Bosch DIVAR IP 3000 是一款 3000 系列视频录像机。

Bosch Video Streaming Gateway（VSG）中存在访问控制错误漏洞，

该漏洞源于程序缺少身份验证。攻击者可利用该漏洞检索和设置 Video Streaming Gateway 的配置数据，影响实时和被录制的视频数据的保密性和可用性。以下产品及版本受到影响：

- Bosch Video Streaming Gateway 6.45 版本至 6.45.08 版本
- Bosch Video Streaming Gateway 6.44 版本至 6.44.022 版本
- Bosch Video Streaming Gateway 6.43 版本至 6.43.0023 版本
- Bosch Video Streaming Gateway 6.42.10 及之前版本
- Bosch DIVAR IP 2000 3.62.0019 及之前版本（设备防火墙的 8023 端口被打开并安装有受影响的 VSG）
- Bosch DIVAR IP 3000（安装有受影响的 VSG）
- Bosch DIVAR IP 5000 3.80.0039 及之前版本（设备防火墙的 8023 端口被打开并安装有受影响的 VSG）
- Bosch DIVAR IP 7000（安装有受影响的 VSG）
- Bosch DIVAR IP all-in-one 5000（安装有受影响的 VSG）

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html

11. FasterXML jackson-databind 代码问题漏洞（CNNVD-202002-354）

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。

FasterXML jackson-databind 2.0.0 版本至 2.9.10.2 版本中存在代码问题漏洞，该漏洞源于程序缺少 xbean-reflect/JNDI 黑名单类。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://github.com/FasterXML/jackson-databind/issues/2620

12. LPAR2RRD 操作系统命令注入漏洞（CNNVD-202002-871）

LPAR2RRD 是一款 CPU（中央处理器）监控工具。

LPAR2RRD 3.5 及之前版本中存在安全漏洞，该漏洞源于程序没有对 web GUI 参数进程输入清理。远程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，补丁获取链接：

http://www.lpar2rrd.com/note453-01.htm

13. **Django SQL 注入漏洞（CNNVD-202002-011）**

Django 是 Django 基金会的一套基于 Python 语言的开源 Web 应用框架。该框架包括面向对象的映射器、视图系统、模板系统等。

Django 1.11.28 之前的 1.11 版本、2.2.10 之前的 2.2 版本和 3.0.3 之前的 3.0 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://docs.djangoproject.com/en/3.0/releases/security/

1.4.2 高危漏洞实例

本月高危漏洞共 473 个，其中重点漏洞实例如表 6 所示。

表 6 2020 年 2 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-202002-1109	Sympa	Foxit Reader 和 PhantomPDF 资源管理错误漏洞（CNNVD-202002-435）
		CNNVD-202002-455	Siemens	
		CNNVD-202002-202	Qualcomm	
		CNNVD-202002-204		
		CNNVD-202002-206		
		CNNVD-202002-041	Python	
		CNNVD-202002-1021	ProFTPD	
		CNNVD-202002-175	Percona	
		CNNVD-202002-540	Microsoft	
		CNNVD-202002-940	IBM	
		CNNVD-202002-736	Huawei	
		CNNVD-202002-361	Google	
		CNNVD-202002-364		
		CNNVD-202002-390		
		CNNVD-202002-1113		
		CNNVD-202002-1119		
		CNNVD-202002-435	Foxit	
		CNNVD-202002-436		
		CNNVD-202002-446		
		CNNVD-202002-447		
		CNNVD-202002-449		
		CNNVD-202002-303	Cisco	
		CNNVD-202002-304		
		CNNVD-202002-305		
		CNNVD-202002-1238		
		CNNVD-202002-626	Adobe	
		CNNVD-202002-632		
		CNNVD-202002-637		
		CNNVD-202002-640		
2	注入	CNNVD-202002-472	Symantec	Symantec Endpoint Protection 和 Small Business Edition 注入漏洞（CNNVD-202002-472）
		CNNVD-202002-1204	Druva	

3	信息泄露	CNNVD-202002-094	Squid	Lenovo XClarity Administrator 信息泄露漏洞（CNNVD-202002-809）
		CNNVD-202002-112	GitLab	
		CNNVD-202002-124		
		CNNVD-202002-295	SUSE	
		CNNVD-202002-412	Huawei	
		CNNVD-202002-416		
		CNNVD-202002-429	Secom	
		CNNVD-202002-487	Apache 软件基金会	
		CNNVD-202002-648	Aruba Networks	
		CNNVD-202002-787	aiCorporation	
		CNNVD-202002-809	Lenovo	
		CNNVD-202002-1002	VMware	
		CNNVD-202002-1063	Atos	
		CNNVD-202002-1069	JetBrains	
		CNNVD-202002-1135	BuddyPress	
4	信任管理问题	CNNVD-202002-1115	Moxa	Cisco NX-OS Software 信任管理问题漏洞（CNNVD-202002-1221）
		CNNVD-202002-1116		
		CNNVD-202002-1221	Cisco	
5	数据伪造问题	CNNVD-202002-065	Nextcloud	Nextcloud Server 数据伪造问题漏洞（CNNVD-202002-065）
6	输入验证错误	CNNVD-202002-019	TP-Link	Google Chrome 输入验证错误漏洞（CNNVD-202002-376）
		CNNVD-202002-044	IBM	
		CNNVD-202002-087	Squid	
		CNNVD-202002-127	Cisco	
		CNNVD-202002-128		
		CNNVD-202002-987		
		CNNVD-202002-989		
		CNNVD-202002-1240		
		CNNVD-202002-170	F5	
		CNNVD-202002-186	Dell	
		CNNVD-202002-199	Qualcomm	
		CNNVD-202002-207		
		CNNVD-202002-211		
		CNNVD-202002-376	Google	
		CNNVD-202002-386		
		CNNVD-202002-399		
		CNNVD-202002-434	Foxit	
		CNNVD-202002-473	Kinetica	

		CNNVD-202002-496	Microsoft	
		CNNVD-202002-499		
		CNNVD-202002-506		
		CNNVD-202002-538		
		CNNVD-202002-541		
		CNNVD-202002-686	IKTeam	
		CNNVD-202002-687	Synergy Systems & Solutions	
		CNNVD-202002-718	SAP	
		CNNVD-202002-720		
		CNNVD-202002-727	HP	
		CNNVD-202002-737	Huawei	
		CNNVD-202002-873		
		CNNVD-202002-811	Combodo	
		CNNVD-202002-822		
		CNNVD-202002-816	Istio	
7	授权问题	CNNVD-202002-038	D-Link	Red Hat Undertow 授权问题漏洞（CNNVD-202002-1245）
		CNNVD-202002-1073		
		CNNVD-202002-1074		
		CNNVD-202002-111	GitLab	
		CNNVD-202002-185	Dell	
		CNNVD-202002-454	Siemens	
		CNNVD-202002-457	Symantec	
		CNNVD-202002-458		
		CNNVD-202002-459		
		CNNVD-202002-475	Ammyy	
		CNNVD-202002-685	Istio	
		CNNVD-202002-999	VMware	
		CNNVD-202002-1009	Cisco	
		CNNVD-202002-1101	Centreon	
		CNNVD-202002-1120	Moxa	
		CNNVD-202002-1245	Red Hat	
8	权限许可和访问控制问题	CNNVD-202002-975	Cisco	Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-202002-975）
9	路径遍历	CNNVD-202002-017	CIRCL	Avaya Equinox Management 路径遍历漏洞（CNNVD-202002-131
		CNNVD-202002-095	1up	
		CNNVD-202002-109	GitLab	
		CNNVD-202002-234	Bosch	

		CNNVD-202002-1104	DNN	9）
		CNNVD-202002-1319	Avaya	
10	跨站请求伪造	CNNVD-202002-036	D-Link	Palo Alto Networks Expedition Migration Tool 跨站请求伪造漏洞（CNNVD-202002-731）
		CNNVD-202002-107	IBM	
		CNNVD-202002-159	Bestwebsoft	
		CNNVD-202002-653	Atlassian	
		CNNVD-202002-654		
		CNNVD-202002-670	CloudBees	
		CNNVD-202002-731	Palo Alto Networks	
		CNNVD-202002-893	Real Estate Connected	
		CNNVD-202002-896	Mozilla 基金会	
		CNNVD-202002-962	SilverStripe	
		CNNVD-202002-979	Cisco	
		CNNVD-202002-1105	MIELE	
		CNNVD-202002-1157	Honeywell	
		CNNVD-202002-1196	Supsystic	
		CNNVD-202002-1273	Cloud Foundry 基金会	
11	加密问题	CNNVD-202002-043	IBM	IBM Security Directory Server 加密问题漏洞（CNNVD-202002-043）
		CNNVD-202002-692		
		CNNVD-202002-1147		
12	缓冲区错误	CNNVD-202002-086	Squid	Android 缓冲区错误漏洞（CNNVD-202002-366）
		CNNVD-202002-099	ipmitool	
		CNNVD-202002-130	Cisco	
		CNNVD-202002-132	ClamAV	
		CNNVD-202002-200	Qualcomm	
		CNNVD-202002-210		
		CNNVD-202002-363	Google	
		CNNVD-202002-366		
		CNNVD-202002-377		
		CNNVD-202002-388		
		CNNVD-202002-397		
		CNNVD-202002-400		
		CNNVD-202002-401		
		CNNVD-202002-402		
		CNNVD-202002-407		
		CNNVD-202002-1192		
		CNNVD-202002-437	Foxit	

		CNNVD-202002-438		
		CNNVD-202002-439		
		CNNVD-202002-440		
		CNNVD-202002-441		
		CNNVD-202002-443		
		CNNVD-202002-444		
		CNNVD-202002-493	Microsoft	
		CNNVD-202002-510		
		CNNVD-202002-528		
		CNNVD-202002-566		
		CNNVD-202002-572		
		CNNVD-202002-577		
		CNNVD-202002-579		
		CNNVD-202002-580		
		CNNVD-202002-585		
		CNNVD-202002-595		
		CNNVD-202002-587	Adobe	
		CNNVD-202002-605		
		CNNVD-202002-606		
		CNNVD-202002-607		
		CNNVD-202002-608		
		CNNVD-202002-609		
		CNNVD-202002-610		
		CNNVD-202002-611		
		CNNVD-202002-612		
		CNNVD-202002-613		
		CNNVD-202002-614		
		CNNVD-202002-615		
		CNNVD-202002-616		
		CNNVD-202002-617		
		CNNVD-202002-618		
		CNNVD-202002-619		
		CNNVD-202002-620		
		CNNVD-202002-621		
		CNNVD-202002-622		
		CNNVD-202002-623		
		CNNVD-202002-624		
		CNNVD-202002-631		
		CNNVD-202002-639		
		CNNVD-202002-642		
		CNNVD-202002-733	Huawei	
		CNNVD-202002-745	netsurf-browser	

		CNNVD-202002-797	PCRE	
		CNNVD-202002-826	Accusoft	
		CNNVD-202002-909	Netsurf-browser	
		CNNVD-202002-910	IBM	
		CNNVD-202002-914	Netsurf-browser	
		CNNVD-202002-1020	ProFTPD	
		CNNVD-202002-1023	Samsung	
		CNNVD-202002-1060	Patriot	
		CNNVD-202002-1111	Pure-FTPd	
		CNNVD-202002-1137	Moxa	
13	后置链接	CNNVD-202002-542	Microsoft	Microsoft Windows User Profile Service 后置链接漏洞（CNNVD-202002-542）
14	格式化字符串错误	CNNVD-202002-131	Cisco	Cisco IOS XR 格式化字符串错误漏洞（CNNVD-202002-131）
		CNNVD-202002-1127	Moxa	
15	访问控制错误	CNNVD-202002-080	Nextcloud	Nextcloud Server 访问控制错误漏洞（CNNVD-202002-080）
		CNNVD-202002-714	SAP	
		CNNVD-202002-866	ABB	
		CNNVD-202002-1045	openHAB	
		CNNVD-202002-1114	Moxa	
		CNNVD-202002-1140		
		CNNVD-202002-1289	Tonnet	
16	代码问题	CNNVD-202002-033	SysJust	CloudBees Jenkins NUnit Plugin 代码问题漏洞（CNNVD-202002-668）
		CNNVD-202002-146	Greenbone Networks	
		CNNVD-202002-152	Atlassian	
		CNNVD-202002-158		
		CNNVD-202002-431	libgd	
		CNNVD-202002-550	Microsoft	
		CNNVD-202002-668	CloudBees	
		CNNVD-202002-675		
		CNNVD-202002-677		
		CNNVD-202002-679		
		CNNVD-202002-729	Palo Alto Networks	
		CNNVD-202002-860	O-dyn	

		CNNVD-202002-961	Western Digital	
		CNNVD-202002-997	Cisco	
		CNNVD-202002-1047	Trend Micro	
		CNNVD-202002-1061	Dell	
		CNNVD-202002-1068	Open-Xchange	
17	操作系统命令注入	CNNVD-202002-052	Fortinet	NEC Aterm WF1200C、Aterm WG1200CR 和 Aterm WG2600HS 操作系统命令注入漏洞（CNNVD-202002-1004）
		CNNVD-202002-451	Moxa	
		CNNVD-202002-1118		
		CNNVD-202002-1122		
		CNNVD-202002-849	Kaseya	
		CNNVD-202002-868	Codecov	
		CNNVD-202002-996	NEC	
		CNNVD-202002-1003		
		CNNVD-202002-1004		
		CNNVD-202002-1187	Druva	
		CNNVD-202002-1236	Cisco	
		CNNVD-202002-1239		
		CNNVD-202002-1242		
18	SQL 注入	CNNVD-202002-030	SysJust	Progress Software MOVEit Transfer SQL 注入漏洞（CNNVD-202002-796）
		CNNVD-202002-247	NetCracker	
		CNNVD-202002-355	TestLink	
		CNNVD-202002-430	xnau	
		CNNVD-202002-796	Progress Software	
		CNNVD-202002-1005	IBM	
		CNNVD-202002-1029	Red Gate	

1. Foxit Reader 和 PhantomPDF 资源管理错误漏洞（CNNVD-202002-435）

Foxit Reader for Windows 和 Foxit PhantomPDF for Windows 都是中国福昕（Foxit）公司的一款基于 Windows 平台的 PDF 文档阅读器。

Foxit Reader 9.7.0.29478 及之前版本（Windows 平台）和 PhantomPDF 9.7.0.29455 及之前版本（Windows 平台）中存在资源管理错

误漏洞，该漏洞源于在对对象执行操作之前程序没有验证该对象是否存在。攻击者可借助恶意的页面或文件利用该漏洞在当前进程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://www.foxitsoftware.com/support/security-bulletins.php

2. Symantec Endpoint Protection 和 Small Business Edition 注入漏洞（CNNVD-202002-472）

Symantec Endpoint Protection（SEP）和 Symantec Endpoint Protection Small Business Edition（SEP SBE）都是美国赛门铁克（Symantec）公司的产品。Symantec Endpoint Protection 是一套防病毒软件。该软件可跨物理和虚拟系统提供安全防护功能。Symantec Endpoint Protection Small Business Edition 是一套适用于中小企业的端点安全防护软件。

Symantec SEP 14.2 RU2 MP1 之前版本和 SEP SBE 14.2.5569.2100 之前版本中存在注入漏洞。攻击者可利用该漏洞执行自己的代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.symantec.com/us/en/article.SYMSA1505.html

3. Lenovo XClarity Administrator 信息泄露漏洞（CNNVD-202002-809）

Lenovo XClarity Administrator（LXCA）是中国联想（Lenovo）公司的一套集中式资源管理解决方案。该产品能够为服务器、存储、

网络交换机等提供无代理硬件管理功能。

Lenovo LXCA 2.6.6 之前版本中存在信息泄露漏洞。攻击者利用该漏洞未经认证，访问一些配置文件，例如用户名、IP 地址、被加密的哈希密码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.lenovo.com/us/en/product_security/LEN-29477

4. Cisco NX-OS Software 信任管理问题漏洞（CNNVD-202002-1221）

Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。

Cisco Nexus 3000 Series Switches 和 Nexus 9000 Series Switches（处于 standalone NX-OS 模式下）中的 NX-OS Software 中存在信任管理问题漏洞。远程攻击者可利用该漏洞绕过 BGP MD5 身份验证，与其他 NX-OS 设备建立 BGP 会话。以下产品及版本受到影响：

- NX-OS Software 9.2(1)版本
- NX-OS Software 9.2(2)版本
- NX-OS Software 9.2(3)版本
- NX-OS Software 9.3(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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-nxos-bgpmd5

5. Nextcloud Server 数据伪造问题漏洞（CNNVD-202002-065）

Nextcloud 是德国 Nextcloud 公司的一套开源的自托管文件同步

和共享的通信应用平台。

Nextcloud Server 17.0.1 版本中存在数据伪造问题漏洞。该漏洞源于网络系统或产品未充分验证数据的来源或真实性。攻击者可利用伪造的数据进行攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://nextcloud.com/security/advisory/?id=NC-SA-2020-002

6. Google Chrome 输入验证错误漏洞（CNNVD-202002-376）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 80.0.3987.87 之前版本中的 storage 存在输入验证错误漏洞，该漏洞源于程序没有充分地执行策略。远程攻击者可借助特制的 HTML 页面利用该漏洞绕过网站隔离。

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/2020/02/stable-channel-update-for-desktop.html

7. Red Hat Undertow 授权问题漏洞（CNNVD-202002-1245）

Red Hat Undertow 是美国红帽（Red Hat）公司的一款基于 Java 的嵌入式 Web 服务器，是 Wildfly（Java 应用服务器）默认的 Web 服务器。

Red Hat Undertow 中的 AJP 连接器存在授权问题漏洞。远程攻击者可利用该漏洞读取受影响服务器的 Web 应用程序文件并可能执行代码。

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：

http://undertow.io/

8. Cisco Data Center Network Manager 权限许可和访问控制问题漏洞（CNNVD-202002-975）

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 Data Center Network Manager (DCNM) Release 11.3(1) 之前版本中的 REST API 端点存在权限许可和访问控制问题漏洞，该漏洞源于程序没有进程充分的访问控制验证。远程攻击者可通过使用低权限账户进行身份验证并发送特制的请求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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200219-dcnm-priv-esc

9. Avaya Equinox Management 路径遍历漏洞（CNNVD-202002-1319）

Avaya Equinox Management（iView）是美国 Avaya 公司的一套会议管理解决方案。

Avaya Equinox Management R9.1.9.0 及之前版本中存在路径遍历漏洞。攻击者可利用该漏洞访问远程服务器上受限目录之外的文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://downloads.avaya.com/css/P8/documents/101064450

10. Palo Alto Networks Expedition Migration Tool 跨站请求伪造漏

洞（CNNVD-202002-731）

Palo Alto Networks Expedition Migration Tool 是美国 Palo Alto Networks 公司的一款安全策略（配置）迁移工具。

Palo Alto Networks Expedition Migration Tool 1.1.51 及之前版本中存在跨站请求伪造漏洞，该漏洞源于没有充分地进行跨站请求伪造保护。远程攻击者可利用该漏洞执行管理员操作。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://security.paloaltonetworks.com/CVE-2020-1977

11. IBM Security Directory Server 加密问题漏洞

（CNNVD-202002-043）

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 6.4.0.0 及之后版本（6.4.0.20 版本已修复）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/1288660

12. Android 缓冲区错误漏洞（CNNVD-202002-366）

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 packet_fragmenter.cc 文件的‘reassemble_and_dispa

tch’函数存在缓冲区错误漏洞，该漏洞源于错误的边界计算。远程攻击者可利用该漏洞执行代码。以下产品及版本受到影响：

- Android 8.0 版本
- Android 8.1 版本
- Android 9 版本
- Android 10 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/2020-02-01

13. Microsoft Windows User Profile Service 后置链接漏洞

（CNNVD-202002-542）

Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。

Microsoft Windows User Profile Service 中存在提权漏洞，该漏洞源于程序处理符号链接不当。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提升权限，删除文件和文件夹。以下产品及版本受到影响：

- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 10 版本 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 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-2020-0730

14. Cisco IOS XR 格式化字符串错误漏洞（CNNVD-202002-131）

Cisco IOS XR 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XR 中的 Cisco Discovery Protocol 实现存在格式化字符串错误漏洞，该漏洞源于程序没有正确验证输入的字符串。攻击者可通过发送恶意的 Cisco Discovery Protocol 数据包利用该漏洞以管

理权限执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce

15. Nextcloud Server 访问控制错误漏洞（CNNVD-202002-080）

Nextcloud 是德国 Nextcloud 公司的一套开源的自托管文件同步和共享的通信应用平台。

Nextcloud Server 14.0.4 版本中存在访问控制错误漏洞。攻击者可借助特制的请求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://nextcloud.com/security/advisory/?id=NC-SA-2019-003

16. CloudBees Jenkins NUnit Plugin 代码问题漏洞

（CNNVD-202002-668）

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。

CloudBees Jenkins 中的 NUnit Plugin 0.25 及之前版本存在代码问题漏洞，该漏洞源于程序没有配置 XML 解析器来防止 XML 外部实体攻击。攻击者可利用该漏洞获取敏感信息，进行服务器端请求伪造或造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://jenkins.io/security/advisory/2020-02-12/

17. NEC Aterm WF1200C、Aterm WG1200CR 和 Aterm WG2600HS 操作系统命令注入漏洞（CNNVD-202002-1004）

NEC Aterm WF1200C 等都是日本电气（NEC）公司的一款无线路由器。

使用 1.2.1 及之前版本固件的 NEC Aterm WF1200C、使用 1.2.1 及之前版本固件 Aterm WG1200CR 和使用 1.3.2 及之前版本版本固件的 Aterm WG2600HS 中存在操作系统命令注入漏洞。攻击者可借助 UPnP 功能利用该漏洞以 root 权限执行任意操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://jvndb.jvn.jp/en/contents/2020/JVNDB-2020-000016.html

18. Progress Software MOVEit Transfer SQL 注入漏洞（CNNVD-202002-796）

Progress Software MOVEit Transfer 是美国 Progress Software 公司的一套文件传输软件。

Progress Software MOVEit Transfer 2019.1.4 之前的 2019.1 版本和 2019.2.1 之前的 2019.2 版本中的 REST API 存在 SQL 注入漏洞。攻击者可利用该漏洞访问 MOVEit Transfer 数据库，并可能推测出数据库的结构和内容，执行 SQL 语句。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://community.ipswitch.com/s/article/MOVEit-Transfer-Security-Vulnerabilities-Feb-2020

二、接报漏洞情况

本月接报漏洞 1230 个，其中信息技术产品漏洞（通用型漏洞）83 个，网络信息系统漏洞（事件型漏洞）1147 个。

表 7 2020 年 2 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	407
2	上海斗象信息科技有限公司	345
3	内蒙古洞明科技有限公司	159
4	北京华云安信息技术有限公司	75
5	太极计算机股份有限公司	65
6	山东新潮信息技术有限公司	52
7	北京圣博润高新技术股份有限公司	29
8	西安四叶草信息技术有限公司	20
9	浙江大华技术股份有限公司	12
10	北京数字观星科技有限公司	10
11	深信服电子科技有限公司	10
12	北京云测信息技术有限公司	8
13	国防科技大学	6
14	个人	7
15	北京国舜科技股份有限公司	5
16	上海安识网络科技有限公司	4
17	北京神州绿盟科技有限公司	4
18	西安交大捷普网络科技有限公司	2

19	北京山石网科信息技术有限公司	2
20	北京云测信息科技有限公司	2
21	北京长亭未来科技有限公司	2
22	北京智游网安科技有限公司	1
23	上海安几科技有限公司	1
24	中国工商银行安全攻防实验室	1
25	北京邮电大学	1
报送总计		1230

三、重大漏洞预警

3.1 思科 CDP 设备多个安全漏洞情况的通报

近日，国家信息安全漏洞库（CNNVD）收到关于思科 CDP 设备多个安全漏洞情况的报送，包括思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、CVE-2020-3111）等多个漏洞。成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。思科 Firepower 1000 Series、IOS XRv 9000 Router、Nexus 1000V Switch、IP Conference Phone 7832、Video Surveillance 8000 Series IP Camera 等多款设备均受此漏洞影响。目前，思科官方已发布漏洞补丁修复了漏洞，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

思科公司是美国一家网络解决方案供应商，CDP 是思科（Cisco）专有的第二层（数据链路层）网络协议，主要用来对本地连接的思科设备进行信息获取。几乎所有的思科产品，包括交换机、路由器、IP 电话和摄像头等，都实现了 CDP 协议，且这些设备出厂时均默认启用 CDP。

1、思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）：

思科视频监控 8000 系列 IP 摄像头的 CDP 协议实现在解析数据包中的 DeviceID 字段时，存在堆溢出漏洞。通过利用此漏洞，攻击者可以对目标设备实施远程代码执行或拒绝服务攻击。

2、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、CVE-2020-3111）

思科 VoIP 电话的 CDP 协议实现在解析 CDP 数据包中的 PortID 字段时，存在栈溢出漏洞。通过利用此漏洞，攻击者可以对目标设备实施远程代码执行或拒绝服务攻击。

3、思科 IOS-XR CDP 格式化字符串漏洞（CNNVD-202002-131、CVE-2020-3118）

思科 IOS XR 的 CDP 协议实现，在解析 CDP 请求包中的某些字符串字段时（比如设备 ID、端口 ID 等），存在格式化字符串漏洞。通过利用此漏洞，攻击者可以在目标路由器上执行任意代码，获取系统权限。

4、思科 NX-OS CDP 远程代码执行漏洞（CNNVD-202002-130、CVE-2020-3119）

运行有思科 NX-OS 软件的设备的 CDP 协议实现，在解析含有 PoE（Power over Ethernet）请求字段的 CDP 数据包时，存在栈溢出漏洞。通过利用此漏洞，攻击者可以在目标交换机上执行任意代码，获取系统权限。

5、思科 FXOS、IOS XR、NX-OS CDP 拒绝服务漏洞（CNNVD-202002-129、CVE-2020-3120）

运行有思科 FXOS、IOS XR 或 NX-OS 软件的设备，其 CDP 协议实现存在拒绝服务漏洞。通过利用此漏洞，攻击者可以对运行有这些软件的目标设备进行拒绝服务攻击。

危害影响

成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。思科 Firepower 1000 Series、IOS XRv 9000 Router、Nexus 1000V Switch、IP Conference Phone 7832、Video Surveillance 8000 Series IP Camera 等多款设备均受此漏洞影响，具体如下：

序号	类型	型号
1	路由器	ASR 9000 Series Aggregation Services Routers Carrier Routing System (CRS) Firepower 1000 Series Firepower 2100 Series Firepower 4100 Series Firepower 9300 Security Appliances IOS XRv 9000 Router White box routers running Cisco IOS XR
2	交换机	Nexus 1000 Virtual Edge Nexus 1000V Switch Nexus 3000 Series Switches

		Nexus 5500 Series Switches Nexus 5600 Series Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Fabric Switches MDS 9000 Series Multilayer Switches Network Convergence System (NCS) 1000 Series Network Convergence System (NCS) 5000 Series Network Convergence System (NCS) 540 Routers Network Convergence System (NCS) 5500 Series Network Convergence System (NCS) 560 Routers Network Convergence System (NCS) 6000 Series UCS 6200 Series Fabric Interconnects UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects
3	IP 电话	IP Conference Phone 7832 IP Conference Phone 8832 IP Phone 6800 Series IP Phone 7800 Series

		IP Phone 8800 Series IP Phone 8851 Series Unified IP Conference Phone 8831 Wireless IP Phone 8821 Wireless IP Phone 8821-EX
4	IP 摄像头	Video Surveillance 8000 Series IP Cameras

修复建议

目前，思科官方已发布漏洞补丁修复了漏洞，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://tools.cisco.com/security/center/publicationListing.x

3.2 微软多个安全漏洞的通报

近日，微软官方发布了用于修复 101 个安全漏洞的公告，包括 Windows 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）、Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）、Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）；Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681；CNNVD-202002-538、CVE-2020-0734；CNNVD-202002-646、CVE-2020-0817）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、Microsoft Office、Edge、Internet Explorer、Microsoft Exchange Server、Microsoft Surface Hub、ChakraCore 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 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）

漏洞简介：Windows 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通过提升权限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。

2、Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）

漏洞简介：Microsoft Windows 在处理.LNK 文件过程中存在一个远程执行代码漏洞。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。攻击者可能会向用户发送包含恶意 .LNK 文件和关联的恶意二进制文件的可移除驱动器或远程共享。当用户在 Windows 资源管理器中打开此驱动器（或远程共享），或打开可分

析 .LNK 文件的其他任何应用程序时，攻击者即可在目标系统上执行代码。

3、Microsoft Internet Explorer 内存破坏漏洞（CNNVD-202001-876、CVE-2020-0674）

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。

4、Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681；CNNVD-202002-538、CVE-2020-0734；CNNVD-202002-646、CVE-2020-0817）

漏洞简介： Windows 远程桌面客户端中存在多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。

5、Media Foundation 内存破坏漏洞（CNNVD-202002-528、CVE-2020-0738）

漏洞简介：当 Windows Media Foundation 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。

6、Microsoft ChakraCore 和 Edge 内存破坏漏洞（CNNVD-202002-579、CVE-2020-0710；CNNVD-202002-566、CVE-2020-0711；CNNVD-202002-580、CVE-2020-0712；CNNVD-202002-572、CVE-2020-0713）

漏洞简介：Microsoft Edge (EdgeHTML-based)和 ChakraCore 中存在远程执行代码漏洞。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。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。

7、Microsoft Excel 资源管理错误漏洞（CNNVD-202002-585、CVE-2020-0759）

漏洞简介：Microsoft Excel 中存在资源管理错误漏洞，该漏洞源于该软件没有正确处理内存中的对象。攻击者可利用该漏洞在当前用户的上下文中运行任意代码。攻击者可利用漏洞安装程序；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、Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 远程执行代码漏洞（CNNVD-202002-496、CVE-2020-0618）

漏洞简介：当 Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 错误地处理页面请求时，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。

安全建议

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 远程执行代码漏洞（CNNVD-202002-510、CVE-2020-0662）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0662
2	Windows LNK 远程执行代码漏洞（CNNVD-202002-544、CVE-2020-0729）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0729
3	Microsoft Internet Explorer 内存破坏	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0674

	漏洞（CNNVD-202001-876、CVE-2020-0674）	
4	Windows 远程桌面客户端远程代码执行漏洞（CNNVD-202002-541、CVE-2020-0681；CNNVD-202002-538、CVE-2020-0734；CNNVD-202002-646、CVE-2020-0817）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0681 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0734 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0817
5	Media Foundation 内存破坏漏洞（CNNVD-202002-528、CVE-2020-0738）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0738
6	Microsoft ChakraCore 和 Edge 内存破坏漏洞（CNNVD-202002-579、CVE-2020-0710；CNNVD-202002-566、CVE-2020-0711；CNNVD-202002-580、CVE-2020-0712；CNNVD-202002-57	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0710 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0711 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0712 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0713

	2、CVE-2020-0713）	
7	Microsoft Excel 资源管理错误漏洞（CNNVD-202002-585、CVE-2020-0759）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0759
8	Microsoft SQL Server 和 Microsoft SQL Server Reporting Services 远程执行代码漏洞（CNNVD-202002-496、CVE-2020-0618）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0618

3.3Apache Tomcat 文件包含漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 Apache Tomcat 文件包含漏洞（CNNVD-202002-1052、CVE-2020-1938）情况的报送。成功利用漏洞的攻击者可以读取 Tomcat 所有 webapp 目录下的任意文件。该漏洞影响包括 Apache Tomcat 9.x、Apache Tomcat 8.x、Apache Tomcat 7.x 、Apache Tomcat 6.x 等多个版本的 Tomcat。目前，Apache 官方已发布公告对修复该漏洞做出说明，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

Tomcat 是 Apache 软件基金会（Apache Software Foundation）

的 Jakarta 项目中的一个核心项目，是 JAVA 中间件服务器之一。Tomcat 中存在一个文件包含漏洞，攻击者利用漏洞可以读取 Tomcat 所有 webapp 目录下的任意文件。如果网站应用提供文件上传的功能，攻击者可以先向服务端上传一个含有恶意 JSP 脚本代码的文件，然后利用漏洞进行文件包含，从而实现代码执行。

在受漏洞影响 Tomcat 版本中，若其开启了 AJP Connector ，且攻击者能够访问 AJP Connector 服务端口的情况下，就会存在被该漏洞利用的风险。Tomcat 的 AJP Connector 默认配置下即为开启状态，因此该漏洞被利用的风险极大。

危害影响

成功利用漏洞的攻击者可以读取 Tomcat 所有 webapp 目录下的任意文件。由于该漏洞影响全版本默认配置下的 Tomcat，因部分 tomcat 版本过于久远，因此该漏洞影响范围至少包含下列版本，但不排除其他版本的 Tomcat。影响版本如下：

Apache Tomcat 9.x < 9.0.31

Apache Tomcat 8.x < 8.5.51

Apache Tomcat 7.x < 7.0.100

Apache Tomcat 6.x

修复建议

目前，Apache 官方已发布公告对修复该漏洞做出说明，可升级至 9.0.31、8.5.51 及 7.0.100 版本对此漏洞进行修复，建议用户及时确

认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

http://tomcat.apache.org/tomcat-9.0-doc/changelog.html#Tomcat_9.0.31_(markt)

要正确修复此漏洞，首先需要确定服务器环境中是否有用到 Tomcat AJP 协议：

1、如果确定未使用 Tomcat AJP 协议，则可以直接将 Tomcat 升级到 9.0.31、8.5.51 或 7.0.100 版本进行漏洞修复。

2、对于确定未使用 Tomcat AJP 协议，但无法进行版本更新、或者是更老版本的用户，可以考虑直接关闭 AJP Connector，或将其监听地址改为仅监听在本机 localhost。具体步骤:

（1）编辑 <CATALINA_BASE>/conf/server.xml，找到如下行（<CATALINA_BASE> 为 Tomcat 的工作目录）：

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

（2）将此行注释掉（或直接删掉此行）：

<!--<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />-->

（3）更改完毕后，重启 Tomcat 即可。

本通报由 CNNVD 技术支撑单位——北京长亭科技有限公司提供支持。