信息安全漏洞通报

2020 年 11 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 11 月份采集安全漏洞共 1297 个。

本月接报漏洞 8623 个，其中信息技术产品漏洞（通用型漏洞）49 个，网络信息系统漏洞（事件型漏洞）8574 个。

重大漏洞预警

微软多个安全漏洞：包括 Windows 权限提升漏洞（CNNVD-202010-1673、CVE-2020-17087）、Windows NFS 远程代码执行漏洞（CNNVD-202011-783、CVE-2020-17051）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。

Drupal 安全漏洞（CNNVD-202011-1698、CVE-2020-13671）：成功利用漏洞的远程攻击者可能获取目标系统或网站的管理权限，执行恶意代码。目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。

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 11 月份新增安全漏洞共 1297 个，从厂商分布来看，Microsoft 公司产品的漏洞数量最多，共发布 111 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 9.71%。本月新增漏洞中，超危漏洞 174 个、高危漏洞 546 个、中危漏洞 545 个、低危漏洞 32 个，相应修复率分别为 84.48%、90.29%、90.46%以及 93.75%。合计 1163 个漏洞已有修复补丁发布，本月整体修复率 89.67%。

截至 2020 年 11 月 30 日，CNNVD 采集漏洞总量已达 154189 个。

1.1 漏洞增长概况

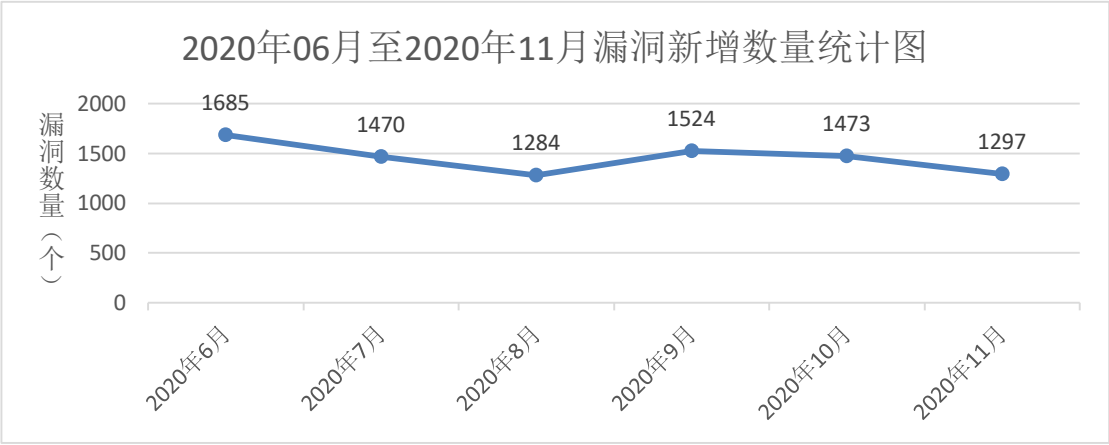

图 1 2020 年 6 月至 2020 年 11 月漏洞新增数量统计图

2020 年 11 月新增安全漏洞 1297 个，与上月（1473 个）相比减少了 11.95%。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 1456 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

11 月厂商漏洞数量分布情况如表 1 所示，Microsoft 公司漏洞达到 111 个，占本月漏洞总量的 8.56%。

表 1　2020 年 11 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	111	8.56%
2	Apple	62	4.78%
3	Cisco	61	4.70%
4	Google	60	4.63%
5	Intel	47	3.62%
6	IBM	43	3.32%
7	Qualcomm	26	2.00%
8	Linux 基金会	22	1.70%
9	CloudBees	21	1.62%
10	Mozilla 基金会	20	1.54%

1.2.2 漏洞产品分布

11 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 54 个。其中 Windows 10 漏洞数量最多，共 52 个，占主流操作系统漏洞总量的 15.20%，排名第一。

表 2　2020 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	Windows 10	52
2	Windows Server 2019	43
3	Windows Server 2016	37

4	Windows Server 2012	32
5	Windows Server 2012 R2	32
6	Windows 8.1	31
7	Windows Rt 8.1	30
8	Android	19
9	Windows Server 2008	18
10	Windows Server 2008 R2	18
11	Windows 7	18
12	Linux Kernel	12
13	Apple Mac OS	0

1.2.3 漏洞类型分布

11 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 9.71%。

表 3 2020 年 11 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	126	9.71%
2	缓冲区错误	108	8.33%
3	代码问题	87	6.71%
4	输入验证错误	84	6.48%
5	授权问题	67	5.17%
6	信息泄露	55	4.24%
7	资源管理错误	39	3.01%
8	访问控制错误	36	2.78%
9	注入	29	2.24%
10	SQL 注入	27	2.08%
11	路径遍历	26	2.00%
12	信任管理问题	22	1.70%
13	跨站请求伪造	19	1.46%
14	命令注入	17	1.31%
15	操作系统命令注入	16	1.23%
16	加密问题	14	1.08%
17	权限许可和访问控制问题	11	0.85%
18	竞争条件问题	8	0.62%
19	数据伪造问题	6	0.46%
20	配置错误	6	0.46%
21	代码注入	5	0.39%
22	日志信息泄露	4	0.31%

23	安全特征问题	4	0.31%
24	后置链接	4	0.31%
25	数字错误	3	0.23%
26	环境问题	3	0.23%
27	参数注入	3	0.23%
28	默认配置问题	2	0.15%
29	格式化字符串错误	1	0.08%
30	其他	464	35.77%

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。11 月漏洞危害等级分布如图 2 所示，其中超危漏洞 174 条，占本月漏洞总数的 13.42%。

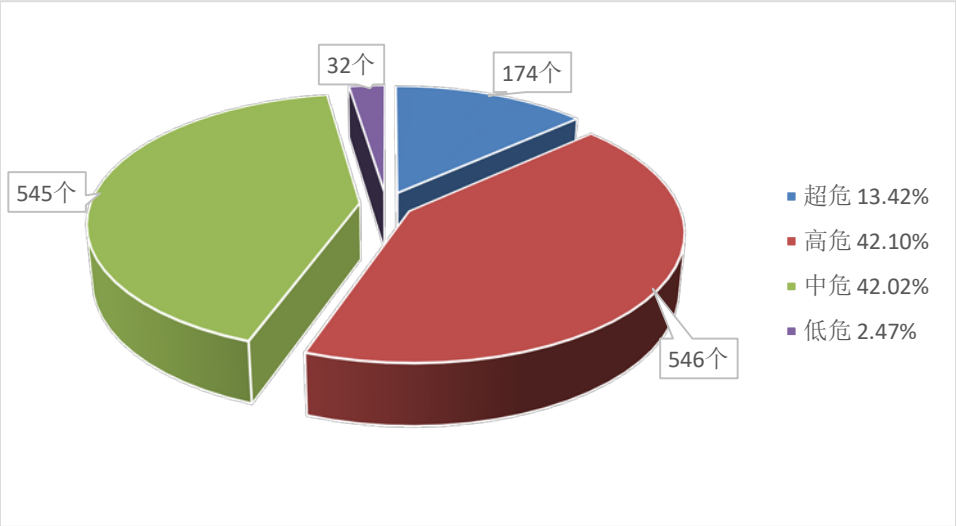

图 2　2020 年 11 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

11 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 93.75%，超危漏洞修复率最低，比例为 84.48%。

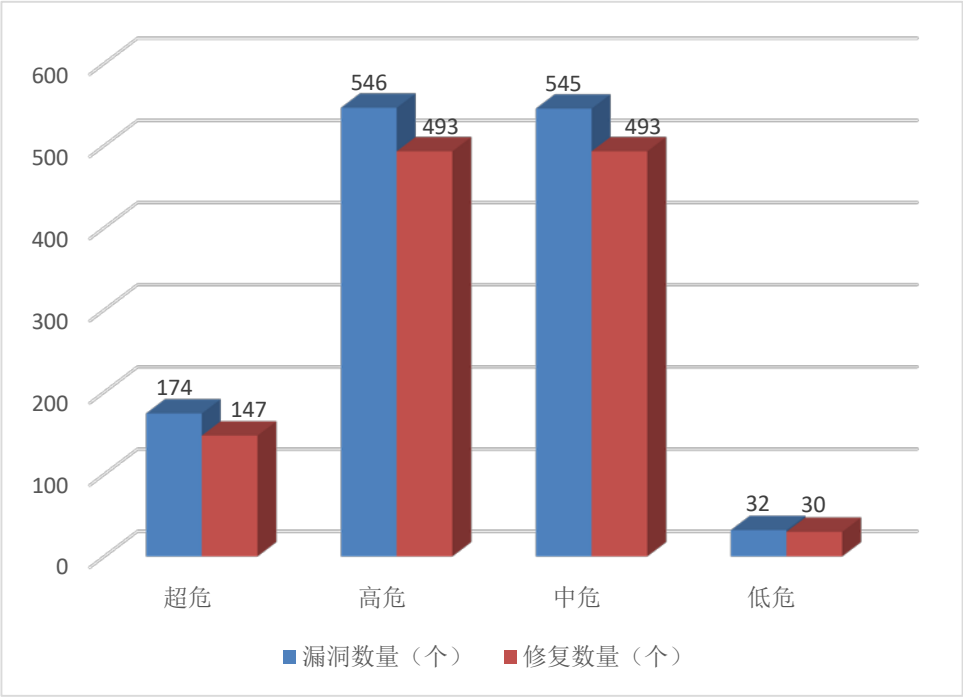

图 3　2020 年 11 月漏洞修复数量统计

1.3.2　厂商修复情况

11 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Microsoft、Apple、Cisco 等十个厂商共 473 条漏洞，占本月漏洞总数的 36.47%，漏洞修复率为 99.37%，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 Microsoft、Apple、Cisco、Google、Intel、IBM、CloudBees、Mozilla 基金会等公司本月漏洞修复率均为 100%，共 470 条漏洞已全部修复。

表 4　2020 年 11 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	Microsoft	111	111	100.00%
2	Apple	62	62	100.00%
3	Cisco	61	61	100.00%
4	Google	60	60	100.00%
5	Intel	47	47	100.00%
6	IBM	43	43	100.00%
7	Qualcomm	26	24	92.31%
8	Linux 基金会	22	21	95.45%

9	CloudBees	21	21	100.00%
10	Mozilla 基金会	20	20	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 174 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 11 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202011-2034	B&r Automation	Micro Focus NetIQ Identity Manager SQL 注入漏洞（CNNVD-202011-1773）
		CNNVD-202011-979	Goodlayers	
		CNNVD-202011-1862	Luckypal	
		CNNVD-202011-1773	Micro Focus	
		CNNVD-202011-1475	Phpgurukul	
		CNNVD-202011-956	Resourcexpress	
		CNNVD-202011-1863	Simplephpscripts	
		CNNVD-202011-1570	Sourcecodester	
		CNNVD-202011-1576		
		CNNVD-202011-1535		
		CNNVD-202011-2088	群晖科技	
2	代码问题	CNNVD-202011-1532	Aviatrix Systems	Cisco Security Manager 代码问题漏洞（CNNVD-202011-1485）
		CNNVD-202011-709	Bitdefender	
		CNNVD-202011-1485	Cisco	
		CNNVD-202011-118	Enhancesoft	
		CNNVD-202011-961	Ivanti	
		CNNVD-202011-706	Microweber 社区	
		CNNVD-202011-156	Qualcomm	
		CNNVD-202011-1531	Sourcecodester	
		CNNVD-202011-1541		
		CNNVD-202011-114	Wordpress 基金会	
		CNNVD-202011-715	Xoonips 团队	
		CNNVD-202011-1391	个人开发者	
		CNNVD-202011-2082		
3	授权问题	CNNVD-202011-1776	Barco	Microsoft Windows Hyper-V 授权问题漏洞（CNNVD-202011-792）
		CNNVD-202011-297	Cloudbees	
		CNNVD-202011-300		
		CNNVD-202011-293		
		CNNVD-202011-1857	Crixp	
		CNNVD-202011-2019	Fujitsu	
		CNNVD-202011-703	Hazelcast	

		CNNVD-202011-1660	Influxdata	
		CNNVD-202011-792	Microsoft	
		CNNVD-202011-1690	Schneider Electric	
		CNNVD-202011-554	Silver Peak	
		CNNVD-202011-1803	Tableau Software	
		CNNVD-202011-1357	个人开发者	
		CNNVD-202011-654		
		CNNVD-202011-1363		
4	操作系统命令注入	CNNVD-202011-1607	Cisco	Ericsson Erlang 操作系统命令注入漏洞（CNNVD-202011-954）
		CNNVD-202011-954	Ericsson	
		CNNVD-202011-302	Saltstack	
		CNNVD-202011-2078	个人开发者	
		CNNVD-202011-2042		
5	缓冲区错误	CNNVD-202011-1651	Cisco	多款 Qualcomm 产品缓冲区错误漏洞（CNNVD-202011-123）
		CNNVD-202011-168	Google	
		CNNVD-202011-1573	Paradox	
		CNNVD-202011-123	Qualcomm	
		CNNVD-202011-153		
		CNNVD-202011-124		
		CNNVD-202011-1568	Real Time Automation	
		CNNVD-202011-1835	Rockwell Automation	
		CNNVD-202011-1876	Schedmd	
		CNNVD-202011-1518	Trend Micro	
		CNNVD-202011-1633	Valvesoftware	
		CNNVD-202011-1799	Winscp 社区	
		CNNVD-202011-2023	Zyxel	
		CNNVD-202011-2062	个人开发者	
		CNNVD-202011-1770	普联	
6	访问控制错误	CNNVD-202011-549	Apache 基金会	Apache Shiro 访问控制错误漏洞 9CNNVD-202011-549)
		CNNVD-202011-1608	Cisco	
		CNNVD-202011-343		
		CNNVD-202011-1692	Endress+hauser	
		CNNVD-202011-1687	Pritunl	
		CNNVD-202011-1671	Schneider Electric	
7	资源管理错误	CNNVD-202011-233	Facebook	Google Chrome 资源管理错误漏洞 (CNNVD-202011-180)
		CNNVD-202011-180	Google	
		CNNVD-202011-1683	Openwrt 社区	
8	输入验证错误	CNNVD-202011-1489	Cisco	Cisco Security Manager 输入验证错误漏洞
		CNNVD-202011-1438	Garmin	

		CNNVD-202011-1437		(CNNVD-202011-1489)
		CNNVD-202011-1435		
		CNNVD-202011-974	Jprichardson	
		CNNVD-202011-159	Qualcomm	
		CNNVD-202011-152		
		CNNVD-202011-154		
		CNNVD-202011-700	Readytalk 团队	
		CNNVD-202011-308	Saltstack	
		CNNVD-202011-972	Sharpred	
		CNNVD-202011-105	Wordpress 基金会	
		CNNVD-202011-208	个人开发者	
		CNNVD-202011-973		
		CNNVD-202011-982		

1. Micro Focus NetIQ Identity Manager SQL 注入漏洞（CNNVD-202011-1773）

Micro Focus NetIQ Identity Manager 是英国 Micro Focus 公司的一套身份认证管理解决方案。该方案为帐户供应、用户自助服务、授权和 Web 服务等提供了基础，并支持数据共享和同步。

NetIQ Identity Manager 4.8 版本至 4.8 SP2 HF1 版本存在安全漏洞，该漏洞源于受到注入漏洞的影响。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.netiq.com/documentation/identity-manager-48/releasenotes_idm4821_apps/data/releasenotes_idm4821_apps.html

2. Cisco Security Manager 代码问题漏洞（CNNVD-202011-1485）

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 Security Manager 存在代码问题漏洞，该漏洞源于受影响的

软件对用户提供的内容进行了不安全的反序列化。攻击者可利用该漏洞可以通过向受影响系统上的特定侦听器发送恶意的序列化 Java 对象来利用这些漏洞。成功的利用可导致在受影响的设备上执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-java-rce-mWJEedcD

3. Microsoft Windows Hyper-V 授权问题漏洞（CNNVD-202011-792）

Microsoft Windows Hyper-V 是美国微软（Microsoft）公司的一款可提供硬件虚拟化的工具。该软件允许创建虚拟硬盘驱动器、虚拟交换机以及许多其他虚拟设备。

Windows Hyper-V 存在授权问题漏洞。以下产品及版本受到影响:Windows 10 Version 1809 for x64-based Systems,Windows 10 Version 1803 for x64-based Systems,Windows Server, version 20H2 (Server Core Installation),Windows Server 2012 R2 (Server Core installation),Windows Server 2012 R2 (Server Core installation),Windows Server 2012 R2,Windows Server 2012 R2,Windows 8.1 for x64-based systems,Windows 8.1 for x64-based systems,Windows Server 2016 (Server Core installation),Windows Server 2016,Windows 10 Version 1607 for x64-based Systems,Windows 10 for x64-based Systems,Windows Server, version 2004 (Server Core installation),Windows 10 Version 2004 for x64-based Systems,Windows

Server, version 1903 (Server Core installation),Windows 10 Version 1903 for x64-based Systems,Windows Server, version 1909 (Server Core installation),Windows 10 Version 1909 for x64-based Systems,Windows Server 2019 (Server Core installation),Windows Server 2019,Windows 10 Version 20H2 for x64-based Systems。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17040

4. **Ericsson Erlang 操作系统命令注入漏洞（CNNVD-202011-954）**

Ericsson Erlang 是瑞典爱立信（Ericsson）公司的一种通用的面向并发的编程语言。

Exposed Erlang 6.5.1 版本存在安全漏洞，该漏洞源于暴露的 Cookie 可能会导致远程命令执行(RCE)攻击。攻击者可利用该漏洞可以使用 cookie 附加到 Erlang 节点上，并在运行 Erlang 节点的系统上运行 OS 级别的命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.couchbase.com/resources/security#VulnerabilityReporting

5. 多款 Qualcomm 产品缓冲区错误漏洞（CNNVD-202011-123）

Qualcomm IPQ6018 等都是美国高通（Qualcomm）公司的一款中央处理器（CPU）产品。

多款 Qualcomm 产品中的 fscanf 存在安全漏洞，该漏洞会导致 堆

栈溢出。受影响产品及版本如下：IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980。

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/samyk/slipstream/commit/19f2f99889150030394493dab455deb3d3a2f341

6. Apache Shiro 访问控制错误漏洞（CNNVD-202011-549）

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 1.7.0 之前版本存在访问控制错误漏洞，该漏洞在 Apache Shiro 与 Spring 一起使用时，特制的 HTTP 请求可能会导致身份验证绕过。

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/rc2cff2538b683d480426393eecf1ce8dd80e052fbef49303b4f47171%40%3Cdev.shiro.apache.org%3E

7. Google Chrome 资源管理错误漏洞（CNNVD-202011-180）

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

Google Chrome 86.0.4240.99 之前的版本中存在资源管理错误漏洞，该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。在使用 Google Chrome 浏览器进行打印后，远程攻击者可以通过精心制作的 HTML 页面利用堆破坏。

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/2020/10/chrome-for-android-update_31.html

8. Cisco Security Manager 输入验证错误漏洞（CNNVD-202011-1489）

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 Security Manager 存在安全漏洞，该漏洞源于在受影响的软件中对静态凭证的保护不够。攻击者可利用该漏洞可以通过查看源代码来利用这个漏洞。成功利用该漏洞可以允许攻击者查看静态凭证，

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-rce-8gjUz9fW

1.4.2 高危漏洞实例

本月高危漏洞共 546 个，其中重点漏洞实例如表 6 所示。

表 6　2020 年 11 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-202011-560	Audimex Ag	IBM Sterling File Gateway SQL 注入漏洞（CNNVD-202011-1381）
		CNNVD-202011-1626	Cisco	
		CNNVD-202011-1396	Ibm	
		CNNVD-202011-1381		
		CNNVD-202011-1459	Ivanti	
		CNNVD-202011-1000	Postgresql	
		CNNVD-202011-1575	Processmaker	
		CNNVD-202011-1706	Red Hat	
		CNNVD-202011-720	Xoonips 团队	
		CNNVD-202011-968	个人开发者	

		CNNVD-202011-1376		
		CNNVD-202011-1552		
		CNNVD-202011-1629		
2	代码问题	CNNVD-202011-1563	Code Projects	Mozilla Firefox MCallGetProperty 代码问题漏洞（CNNVD-202011-717）
		CNNVD-202011-1450		
		CNNVD-202011-1698	Drupal 社区	
		CNNVD-202011-1664	Ibm	
		CNNVD-202011-569	Immuta	
		CNNVD-202011-918	Intel	
		CNNVD-202011-926		
		CNNVD-202011-921		
		CNNVD-202011-977	Ivanti	
		CNNVD-202011-658	Kitabisa	
		CNNVD-202011-1638	Lemocms 社区	
		CNNVD-202011-683	Lg	
		CNNVD-202011-684		
		CNNVD-202011-962	Macdonaldrobinson	
		CNNVD-202011-901	Mcafee	
		CNNVD-202011-899		
		CNNVD-202011-959		
		CNNVD-202011-705	Microweber 社区	
		CNNVD-202011-670	Mit	
		CNNVD-202011-597	Mitsubishi Electric	
		CNNVD-202011-717	Mozilla	
		CNNVD-202011-894	Nvidia	
		CNNVD-202011-1691	Pear	
		CNNVD-202011-817	Sap	
		CNNVD-202011-730		
		CNNVD-202011-1667	Schneider Electric	
		CNNVD-202011-1680		
		CNNVD-202011-1666		
		CNNVD-202011-842		
		CNNVD-202011-1536	Sourcecodester	
		CNNVD-202011-1616	Trend Micro	
		CNNVD-202011-1617		
		CNNVD-202011-805	Wordpress 基金会	
		CNNVD-202011-397	个人开发者	
		CNNVD-202011-966		
		CNNVD-202011-1444		
		CNNVD-202011-1432		
		CNNVD-202011-998		

		CNNVD-202011-276		
		CNNVD-202011-101		
		CNNVD-202011-672	开源	
3	授权问题	CNNVD-202011-602	Apple	Apple Kernel 授权问题漏洞（CNNVD-202011-590）
		CNNVD-202011-590		
		CNNVD-202011-2032	B&r Automation	
		CNNVD-202011-2035		
		CNNVD-202011-949	Bd	
		CNNVD-202011-1604	Broadcom	
		CNNVD-202011-337	Cisco	
		CNNVD-202011-1338	Citrix Systems	
		CNNVD-202011-2022	Devid Espenschied	
		CNNVD-202011-1380	Ibm	
		CNNVD-202011-570	Immuta	
		CNNVD-202011-900	Mersive Technologies	
		CNNVD-202011-599	Mitsubishi Electric	
		CNNVD-202011-1867	Mongodb	
		CNNVD-202011-335	Moxa	
		CNNVD-202011-338		
		CNNVD-202011-916	Palo Alto Networks	
		CNNVD-202011-735	Sap	
		CNNVD-202011-1767	Scratchverifier	
		CNNVD-202011-1817	Security Onion Solutions	
		CNNVD-202011-657	Tenable Network Security	
		CNNVD-202011-1702	Vmware	
		CNNVD-202011-2024	个人开发者	
4	操作系统命令注入	CNNVD-202011-299	Cisco	Cisco Integrated Management Controller 操作系统命令注入漏洞（CNNVD-202011-299）
		CNNVD-202011-1621		
		CNNVD-202011-1337	Citrix Systems	
		CNNVD-202011-737		
		CNNVD-202011-001	Openfind Information Technology	
		CNNVD-202011-915	Palo Alto Networks	
		CNNVD-202011-1632	Tp-link	
		CNNVD-202011-1523	Trend Micro	

		CNNVD-202011-1522		
		CNNVD-202011-1441	Xstream	
		CNNVD-202011-1915	个人开发者	
5	缓冲区错误	CNNVD-202011-194	Adobe	Google Chrome 缓冲区错误漏洞（CNNVD-202011-167）
		CNNVD-202011-2043	Blosc 团队	
		CNNVD-202011-340	Cisco	
		CNNVD-202011-341		
		CNNVD-202011-342		
		CNNVD-202011-1837	Fuji Electric	
		CNNVD-202011-2096	Genvini 组织	
		CNNVD-202011-178	Google	
		CNNVD-202011-174		
		CNNVD-202011-167		
		CNNVD-202011-209		
		CNNVD-202011-1597		
		CNNVD-202011-173		
		CNNVD-202011-172		
		CNNVD-202011-170		
		CNNVD-202011-231		
		CNNVD-202011-1893	Huawei	
		CNNVD-202011-1652	Ibm	
		CNNVD-202011-1771	Imagemagick Studio	
		CNNVD-202011-665	Lightbend	
		CNNVD-202011-2058	Linux 基金会	
		CNNVD-202011-092		
		CNNVD-202011-745	Microsoft	
		CNNVD-202011-743		
		CNNVD-202011-1500	Mozilla 基金会	
		CNNVD-202011-1515		
		CNNVD-202011-699	Netgear	
		CNNVD-202011-1571	Paradox	
		CNNVD-202011-997	Pixar	
		CNNVD-202011-992		
		CNNVD-202011-990		
		CNNVD-202011-988		
		CNNVD-202011-991		
		CNNVD-202011-989		
		CNNVD-202011-1003		
		CNNVD-202011-139	Qualcomm	
		CNNVD-202011-125		
		CNNVD-202011-144		

		CNNVD-202011-146		
		CNNVD-202011-137		
		CNNVD-202011-122		
		CNNVD-202011-2093	Red Hat	
		CNNVD-202011-685	Samsung	
		CNNVD-202011-749	Sap	
		CNNVD-202011-1559	Schneider Electric	
		CNNVD-202011-1556		
		CNNVD-202011-1560		
		CNNVD-202011-1561		
		CNNVD-202011-1639		
		CNNVD-202011-1562		
		CNNVD-202011-1567		
		CNNVD-202011-1564		
		CNNVD-202011-1558		
		CNNVD-202011-1557		
		CNNVD-202011-1644		
		CNNVD-202011-1645		
		CNNVD-202011-1520	Trend Micro	
		CNNVD-202011-606	Wecon Technologies	
		CNNVD-202011-610		
		CNNVD-202011-655	个人开发者	
		CNNVD-202011-1887		
		CNNVD-202011-290		
		CNNVD-202011-1899		
		CNNVD-202011-1765		
		CNNVD-202011-563		
6	访问控制错误	CNNVD-202011-192	Adobe	Cisco IoT Field Network Director 访问控制错误漏洞（CNNVD-202011-1627）
		CNNVD-202011-1627	Cisco	
		CNNVD-202011-1619		
		CNNVD-202011-259		
		CNNVD-202011-212	Gitlab	
		CNNVD-202011-927	Intel	
		CNNVD-202011-963	Macdonaldrobinson	
		CNNVD-202011-796	Microsoft	
		CNNVD-202011-786		
		CNNVD-202011-816		
		CNNVD-202011-791		
		CNNVD-202011-775		
		CNNVD-202011-1434	Prestashop	
		CNNVD-202011-1479	个人开发者	

		CNNVD-202011-1480		
		CNNVD-202011-1858	剑桥大学	
7	资源管理错误	CNNVD-202011-195	Adobe	Microsoft Azure Sphere 资源管理错误漏洞（CNNVD-202011-907）
		CNNVD-202011-184		
		CNNVD-202011-2092	Apple	
		CNNVD-202011-976	Bab Technologie Gmbh	
		CNNVD-202011-1447	Cloudavid	
		CNNVD-202011-171	Google	
		CNNVD-202011-177		
		CNNVD-202011-211		
		CNNVD-202011-176		
		CNNVD-202011-224		
		CNNVD-202011-179		
		CNNVD-202011-175		
		CNNVD-202011-1834	KDE,Apple,Google	
		CNNVD-202011-263	Linux 基金会	
		CNNVD-202011-1793		
		CNNVD-202011-907	Microsoft	
		CNNVD-202011-756		
		CNNVD-202011-1002	Mitsubishi Electric	
		CNNVD-202011-1663		
		CNNVD-202011-585		
		CNNVD-202011-1478	Openjs 基金会	
		CNNVD-202011-986	Pixar	
		CNNVD-202011-987		
		CNNVD-202011-126	Qualcomm	
		CNNVD-202011-155		
		CNNVD-202011-741	Siemens	
		CNNVD-202011-1762	Vmware	
		CNNVD-202011-183	Wago	
		CNNVD-202011-112	Wireshark	
		CNNVD-202011-1910	Zetetic	
8	输入验证错误	CNNVD-202011-190	Adobe	Microsoft SharePoint 输入验证错误漏洞（CNNVD-202011-763）
		CNNVD-202011-605	Apple	
		CNNVD-202011-604		
		CNNVD-202011-608		
		CNNVD-202011-612		
		CNNVD-202011-1777	Barco	
		CNNVD-202011-256	Cisco	
		CNNVD-202011-332		

		CNNVD-202011-1788	Davidtschumperlé Greyc	
		CNNVD-202011-222	Google	
		CNNVD-202011-169		
		CNNVD-202011-1760	Hcl Software	
		CNNVD-202011-1761	Hcl Technologies	
		CNNVD-202011-1759		
		CNNVD-202011-1894	Huawei	
		CNNVD-202011-863	Intel	
		CNNVD-202011-1818	Jingyun	
		CNNVD-202011-1823		
		CNNVD-202011-1794		
		CNNVD-202011-1819		
		CNNVD-202011-1821		
		CNNVD-202011-667	Lightbend	
		CNNVD-202011-884	Microsoft	
		CNNVD-202011-763		
		CNNVD-202011-1814	Mongodb	
		CNNVD-202011-1421	Nagios	
		CNNVD-202011-182	Nexcom	
		CNNVD-202011-181		
		CNNVD-202011-135	Qualcomm	
		CNNVD-202011-148		
		CNNVD-202011-157		
		CNNVD-202011-151		
		CNNVD-202011-145		
		CNNVD-202011-150		
		CNNVD-202011-1836	Rockwell Automation	
		CNNVD-202011-1553	Tobesoft	
		CNNVD-202011-1701	Vmware	
		CNNVD-202011-1407	个人开发者	
		CNNVD-202011-1554		
		CNNVD-202011-691		
		C+C2:C241NNVD-202011-1791		

1. IBM Sterling File Gateway SQL 注入漏洞（CNNVD-202011-1381）

IBM Sterling File Gateway 是美国 IBM 公司的一套文件传输软

件。该软件可整合不同的文件传输活动中心，并帮助基于文件的数据通过因特网实现安全交换。

IBM Sterling File Gateway 存在 SQL 注入漏洞，该漏洞允许攻击者可以发送专门编写的 SQL 语句，这些语句允许攻击者查看、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://www.ibm.com/support/pages/node/6367981

2. Mozilla Firefox MCallGetProperty 代码问题漏洞（CNNVD-202011-717）

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

Firefox 存在安全漏洞，攻击者可利用该漏洞通过 Firefox 的 MCallGetProperty 强制使用释放的内存区域，以触发拒绝服务，并可能运行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2020-49/

3. Apple Kernel 授权问题漏洞（CNNVD-202010-1236）

Apple iOS 是美国苹果（Apple）公司的一套为移动设备所开发的操作系统。

Apple Kernel 中存在授权问题漏洞，该漏洞允许应用程序能够以内核特权执行任意代码。以下产品及版本会受到影响：Apple iPhone 6s 及更高版本, iPod touch 7th generation, iPad Air 2 及更高版本, iPad mini 4 及更高版本。

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/en-us/HT211929

4. Cisco Integrated Management Controller 操作系统命令注入漏洞（CNNVD-202011-299）

Cisco Integrated Management Controller（IMC）是美国思科（Cisco）公司的一套用于对 UCS（统一计算系统）进行管理的软件。该软件支持 HTTP、SSH 访问等，并可对服务器进行开机、关机和重启等操作。

Cisco Integrated Management Controller (IMC) 中的 web UI 存在操作系统命令注入漏洞，该漏洞允许经过身份验证的远程攻击者在底层操作系统级别注入任意代码并执行。

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-CIMC-CIV-pKDBe9x5

5. Google Chrome 缓冲区错误漏洞（CNNVD-202011-167）

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

Google Chrome 86.0.4240.183 之前版本存在安全漏洞，攻击者可能会通过精心制作的 HTML 页面利用堆破坏触发漏洞。

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/2020/11/stable-channel-update-for-desktop.html

6. Cisco IoT Field Network Director 访问控制错误漏洞

（CNNVD-202011-1627）

Cisco IoT Field Network Director（IoT-FND）是美国思科（Cisco）公司的一套端到端的物联网管理系统。该系统具有设备管理、资产跟踪和智能计量等功能。

Cisco IoT Field Network Director 存在访问控制错误漏洞，该漏洞源于 SOAP API 中的授权不足造成的。攻击者可以利用此漏洞，将 SOAP API 请求发送到受影响的设备，这些设备位于其授权域之外。成功的利用可以允许攻击者访问和修改属于不同域的设备上的信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-AUTH-vEypBmmR

7. Microsoft Azure Sphere 资源管理错误漏洞（CNNVD-202011-907）

Microsoft Azure Sphere 是美国微软（Microsoft）公司的一个应用于云环境提供安全防护的设备。

Microsoft Azure Sphere 存在安全漏洞，该漏洞源于 Azure Sphere 未签名导致的代码执行。

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-2020-16970

8. Microsoft SharePoint 输入验证错误漏洞（CNNVD-202011-763）

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与

他人协同工作、组织项目和工作组、搜索人员和信息。

Microsoft SharePoint 存在输入验证错误漏洞。以下产品及版本受到影响:Microsoft SharePoint Server 2010 Service Pack 2,Microsoft SharePoint Server 2019,Microsoft SharePoint Enterprise Server 2013 Service Pack 1,Microsoft SharePoint Enterprise Server 2016。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17016

二、接报漏洞情况

本月接报漏洞 8623 个，其中信息技术产品漏洞（通用型漏洞）49 个，网络信息系统漏洞（事件型漏洞）8574 个。

表 7 2020 年 11 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	4585
2	网神信息技术（北京）股份有限公司	1736
3	北京山石网科信息技术有限公司	474
4	长春嘉诚信息技术股份有限公司	362
5	北京奇虎科技有限公司	208
6	北京微步在线科技有限公司	197
7	北京天地和兴科技有限公司	115
8	内蒙古奥创科技有限公司	95
9	中新网络信息安全股份有限公司	86

10	山东华鲁科技发展股份有限公司	85
11	山东新潮信息技术有限公司	60
12	北京启明星辰信息安全技术有限公司	59
13	西安四叶草信息技术有限公司	59
14	新华三技术有限公司	50
15	北京华云安信息技术有限公司	47
16	杭州迪普科技股份有限公司	32
17	山东云天安全技术有限公司	31
18	北京数字观星科技有限公司	30
19	亚信科技（成都）有限公司	27
20	北京顶象技术有限公司 洞见安全实验室	26
21	中国电子科技网络信息安全有限公司	22
22	杭州海康威视数字技术股份有限公司	22
23	广州锦行网络科技有限公司	20
24	星云博创科技有限公司	19
25	浙江大华技术股份有限公司	16
26	中国电信集团系统集成有限责任公司	14
27	北京邮电大学	14
28	北京锦龙信安科技有限公司	14
29	杭州默安科技有限公司	13
30	北京安华金和科技有限公司	10
31	深圳市魔方安全科技有限公司	10
32	北京天融信网络安全技术有限公司	9

33	中兴通讯	8
34	北京梆梆安全科技有限公司	7
35	北京威努特技术有限公司	6
36	北京华云安信息技术有限公司	5
37	北京中测安华科技有限公司	5
38	绿盟科技集团股份有限公司安全研究部	5
39	上海安识网络科技有限公司	4
40	信息系统安全技术重点实验室	4
41	北京智游网安科技有限公司	4
42	广东东福信息技术有限公司	4
43	深信服科技股份有限公司	4
44	国防科技大学	4
45	上海安几科技有限公司	3
46	个人	2
47	广州竞远安全技术股份有限公司	2
48	美国印第安纳大学伯明顿分校，中国科学院信息工程研究所	2
49	西安交大捷普网络科技有限公司	2
50	中国信息安全测评中心	1
51	信息工程大学	1
52	北京安信天行科技有限公司	1
53	四川大学网络空间安全学院　北京未来安全信息技术有限公司	1
54	北京长亭科技有限公司	1
报送总计		8623

三、重大漏洞预警

3.1 Drupal 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Drupal 安全漏洞（CNNVD-202011-1698、CVE-2020-13671）情况的报送。成功利用漏洞的远程攻击者可能获取目标系统或网站的管理权限，执行恶意代码。Drupal Core 7、8.8、8.9、9.0 各分支版本均受此漏洞影响。目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。

.漏洞介绍

Drupal 是 Drupal 社区的一套使用 PHP 语言开发的开源内容管理系统。Drupal Core 存在安全漏洞，由于 Drupal Core 未正确处理上传文件中的某些文件名，可能导致文件会被错误地解析为其他 MIME 类型，未授权的远程攻击者可通过上传特定文件名的恶意文件利用漏洞执行代码。

.危害影响

成功利用该漏洞的远程攻击者，可获取目标系统或网站的管理权限，执行恶意代码。以下等版本均受此漏洞影响：

Drupal < 7.7.4

Drupal < 8.8.11

Drupal < 8.9.9

Drupal < 9.0.8

注：官方已经停止维护 8.8.x 之前的 Drupal 8 版本。

.修复建议

目前，Drupal 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Drupal Core 产品版本，如受影响，请及时采取修补措施。漏洞修补措施如下：

Drupal 9.0 系列用户，建议更新至 Drupal 9.0.8 版本，链接为 https://www.drupal.org/project/drupal/releases/9.0.8。

Drupal 8.9 系列用户，建议更新至 Drupal 8.9.9 版本，链接为 https://www.drupal.org/project/drupal/releases/8.9.9。

Drupal 8.8 系列用户，建议更新至 Drupal 8.8.11 版本，链接为 https://www.drupal.org/project/drupal/releases/8.8.11。

Drupal 7 系列用户，建议更新至 Drupal 7.74，链接为 https://www.drupal.org/project/drupal/releases/7.74。

3.2 微软多个安全漏洞的的预警

近日，微软官方发布了多个安全漏洞的公告，包括 Windows 权限提升漏洞（CNNVD-202010-1673、CVE-2020-17087）、Windows NFS 远程代码执行漏洞（CNNVD-202011-783、CVE-2020-17051）、Windows

Exchange Server 远程代码执行漏洞（CNNVD-202011-755、CVE-2020-17084）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。

.漏洞介绍

2020 年 11 月 11 日，微软发布了 2020 年 11 月份安全更新，共 112 个漏洞的补丁程序，CNNVD 对这些漏洞进行了收录。本次更新主要涵盖了 Windows 操作系统、IE/Edge 浏览器、Office 组件及 Web Apps、ChakraCore、Exchange 服务器、.Net 框架、Azure DevOps、Windows Defender、Visual Studio 等多个 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，其中部分重要漏洞详情如下：

1、Windows cng.sys 权限提升漏洞（CNNVD-202010-1673、CVE-2020-17087）

漏洞简介：Windows Kernel 中存在一个本地权限提升漏洞，未授权的攻击者通过 诱使用户运行恶意的二进制程序 ,最终造成 权限提升 。

2、Windows NFS 远程代码执行漏洞（CNNVD-202011-783、CVE-2020-17051）

漏洞简介：Windows NFS 是一种网络文件系统，用户可以通过 NFS 访问网络上的文件并将它们像本地文件一样操作。攻击者可以利用此漏洞来访问系统，并远程执行恶意代码。

3、Windows Exchange Server 远程代码执行漏洞（CNNVD-202011-755、CVE-2020-17084）

漏洞简介：Windows Exchange Server 中存在一个远程代码执行漏洞，未授权的远程攻击者通过向 Exchage 服务器发送特制的请求包来进行漏洞利用，利用成功后便可获得服务器完整控制权限。

4、Windows Hyper-V 验证绕过漏洞（CNNVD-202011-792、CVE-2020-17040）

漏洞简介：未授权的远程攻击通过向 Hyper-V 服务器发送特制的请求包来进行漏洞利用，利用成功后便可绕过 Hyper-V 现有的部分安全特性。

由于此次更新，微软并没有透露太多漏洞详情，请用户自行到官方网站查询，官方地址：

https://msrc.microsoft.com/update-guide/en-us

.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。微软官方补丁下载地址：

https://msrc.microsoft.com/update-guide/en-us