国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 10 月 12 日-2020 年 10 月 18 日　　2020 年第 42 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 372 个，其中高危漏洞 124 个、中危漏洞 180 个、低危漏洞 68 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 153 个（占 41%），其中互联网上出现“WordPress Colorbox Lightbox 跨站脚本漏洞、WebBuilder SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 5332 个，与上周（2902 个）环比增加 84%。

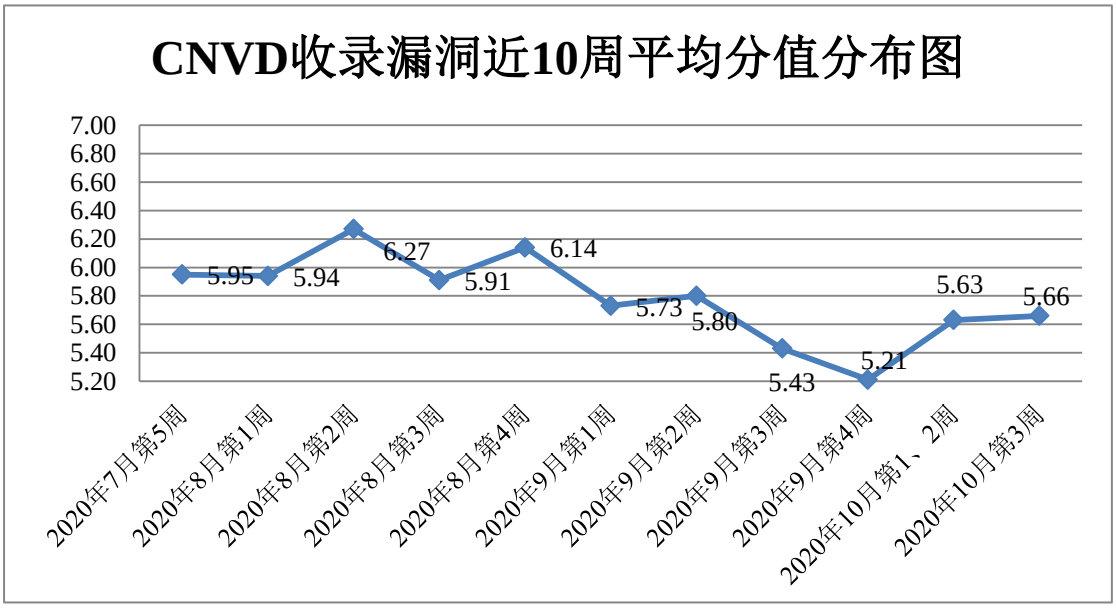

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 24 起，向基础电信企业通报漏洞事件 11 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞

事件 266 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 94 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 29 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

北京信安世纪科技股份有限公司、北京致远互联软件股份有限公司、中国电力工程有限公司、三星（中国）投资有限公司、友讯电子设备（上海）有限公司、中移铁通有限公司智能产品分公司、北京百家互联科技有限公司、西安麦游网络科技有限公司、广东凯格科技有限公司、珠海金山办公软件有限公司、吉林省源晟企业管理有限公司、首岳資訊網路股份有限公司、长沙米拓信息技术有限公司、内蒙古浩海商贸有限公司、北京通王科技有限公司、北京因酷时代科技有限公司、廊坊市极致网络科技有限公司、深圳极速创想科技有限公司、梅州海能科技有限公司、锐捷网络股份有限公司、深圳市吉祥腾达科技有限公司、尚科齐（北京）网络科技有限公司、杭州吉拉科技有限公司、北京网文云科技有限公司、安徽九五信息科技有限公司、上海泛微网络科技股份有限公司、无锡迅诚信息科技有限公司、淄博闪灵网络科技有限公司、三菱电机自动化（中国）有限公司、高通企业管理（上海）有限公司、烽火通信科技股份有限公司、洋葱设计公司、深圳市帝纳达科技有限公司、厦门狮子鱼网络科技有限公司、江苏易安联网络技术有限公司、青岛掌控传媒有限公司、研华科技（中国）有限公司、Panasonic 集团、智睿软件、施耐德（Schneider Electric）、鱼跃 CMS、信呼 OA 办公系统、NETIS SYSTEMS、XiaoCMS、PHPEMS、YYCMS、ShuipFCMS、Foxit 和 ZZCMS。

本周，CNVD 发布了《Microsoft 发布 2020 年 10 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5773

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。长春嘉诚信息技术股份有限公司、国瑞数码零点实验室、山东华鲁科技发展股份有限公司、北京华云安信息技术有限公司、河南灵创电子科技有限公司、山东云天安全技术有限公司、山东道普测评技术有限公司、吉林谛听信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、南京众智维信息科技有限公司、北京机沃科技有限公司、河南信安世纪科技有限公司、内蒙古奥创科技有限公司、浙江安腾信息技术有限公司、北京长亭科技有限公司、京东云安全、长扬科技（北京）有限公司、广州云峰信息科技有限公司、内蒙古中叶信息技术有限责任公司、深圳市魔方安全科技有限公司、安徽长泰信息安全服务有限公司、

北京浩瀚深度信息技术股份有限公司、联想全球安全实验室、中科信息安全共性技术国家工程研究中心有限公司、北京锐服信科技有限公司、山石网科通信技术股份有限公司、郑州云智信安安全技术有限公司、北京惠而特科技有限公司、广州市蓝爵计算机科技有限公司、北京威努特技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、武汉安域信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 5332 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 3905 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
奇安信网神（补天平台）	1794	1794
斗象科技（漏洞盒子）	1712	1712
上海交大	399	399
北京神州绿盟科技有限公司	276	4
哈尔滨安天科技集团股份有限公司	210	0
华为技术有限公司	177	0
北京天融信网络安全技术有限公司	169	4
北京启明星辰信息安全技术有限公司	144	89
中新网络信息安全股份有限公司	121	121
深信服科技股份有限公司	99	0
北京数字观星科技有限公司	75	0
北京奇虎科技有限公司	75	75
中国电信集团系统集成有限责任公司	54	54
西安四叶草信息技术有限公司	23	23
北京知道创宇信息技术股份有限公司	3	0
沈阳东软系统集成工程有限公司	2	2

恒安嘉新(北京)科技股份公司	1	0
长春嘉诚信息技术股份有限公司	288	288
国瑞数码零点实验室	61	61
山东华鲁科技发展股份有限公司	49	49
北京华云安信息技术有限公司	21	21
河南灵创电子科技有限公司	20	20
杭州迪普科技股份有限公司	14	0
山东云天安全技术有限公司	14	14
山东道普测评技术有限公司	13	13
吉林谛听信息技术有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	10	10
南京众智维信息科技有限公司	9	9
北京机沃科技有限公司	8	8
河南信安世纪科技有限公司	8	8
内蒙古奥创科技有限公司	6	6
浙江安腾信息技术有限公司	4	4
北京长亭科技有限公司	4	4
京东云安全	4	4
长扬科技（北京）有限公司	3	3
广州云峰信息科技有限公司	2	2
内蒙古中叶信息技术有限责任公司	2	2
深圳市魔方安全科技有限公司	2	2

安徽长泰信息安全服务有限公司	1	1
北京浩瀚深度信息技术股份有限公司	1	1
联想全球安全实验室	1	1
中科信息安全共性技术国家工程研究中心有限公司	1	1
北京锐服信科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
郑州云智信安安全技术有限公司	1	1
北京惠而特科技有限公司	1	1
广州市蓝爵计算机科技有限公司	1	1
北京威努特技术有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
武汉安域信息安全技术有限公司	1	1
CNCERT 四川分中心	2	2
CNCERT 云南分中心	1	1
个人	501	501
报送总计	6403	5332

本周漏洞按类型和厂商统计

本周，CNVD 收录了 372 个漏洞。应用程序 133 个，WEB 应用 130 个，操作系统 81 个，网络设备（交换机、路由器等网络端设备）16 个，安全产品 6 个，智能设备（物联网终端设备）5 个，数据库 1 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序	133
WEB 应用	130
操作系统	81

网络设备（交换机、路由器等网络端设备）	16
安全产品	6
智能设备（物联网终端设备）	5
数据库	1

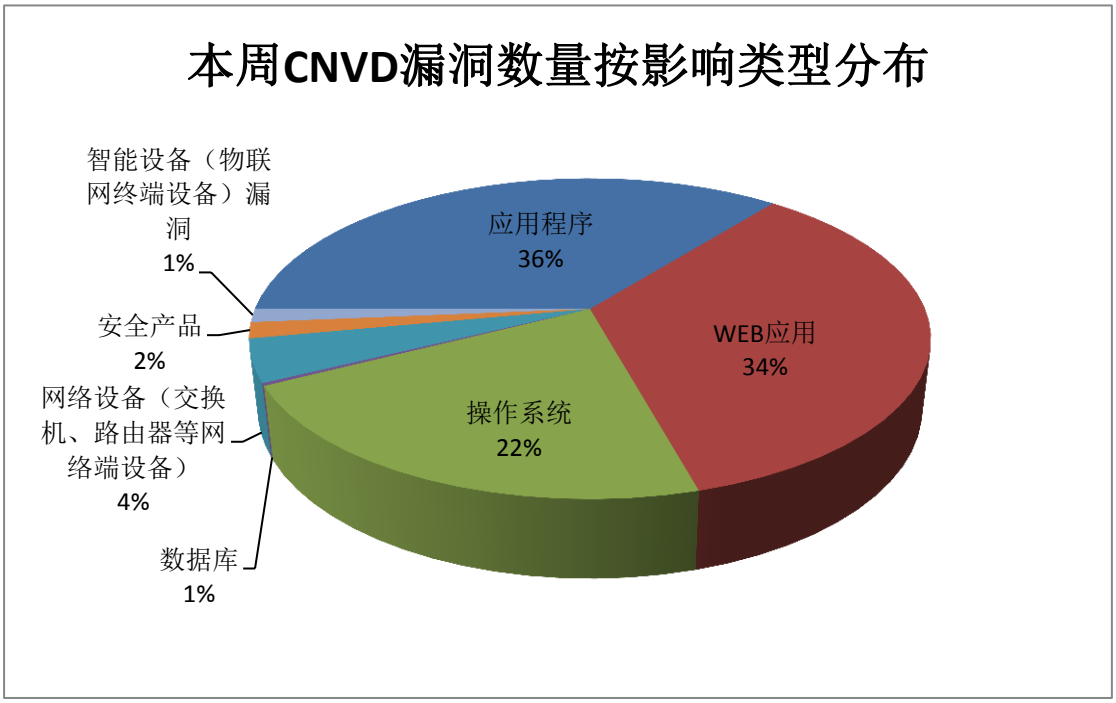

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、IBM 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Google	62	17%
2	Microsoft	25	7%
3	IBM	16	4%
4	CloudBees	12	3%
5	Cisco	12	3%
6	Oracle	10	3%
7	嘉兴想天信息科技有限公司	8	2%
8	Apache	6	2%
9	Moxa	6	2%
10	其他	215	57%

本周行业漏洞收录情况

本周，CNVD 收录了 8 个电信行业漏洞，61 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Google Android 代码问题漏洞（CNVD-2020-55951）、Cisco IOS XE Software 任意代码执行漏洞、LAquis SCADA 越界读取漏洞、Cisco IOS XE 拒绝服务漏洞（CNVD-2020-56629）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

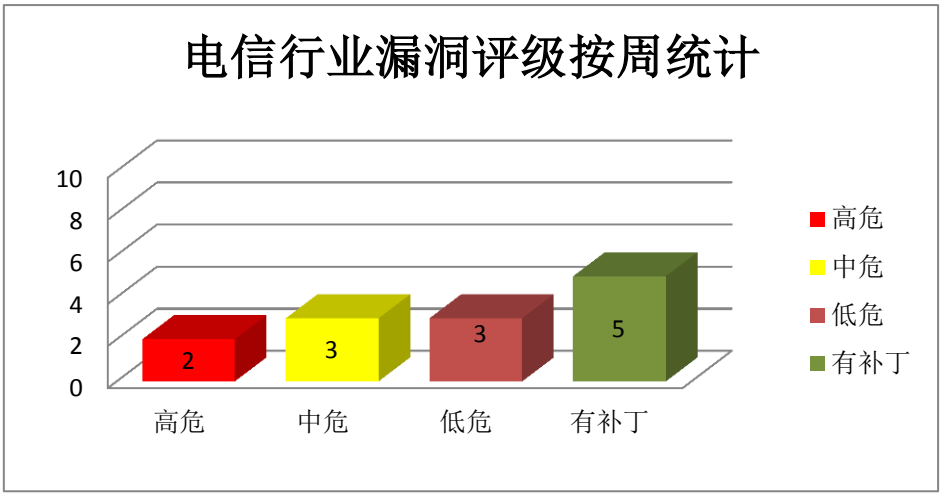

图 3 电信行业漏洞统计

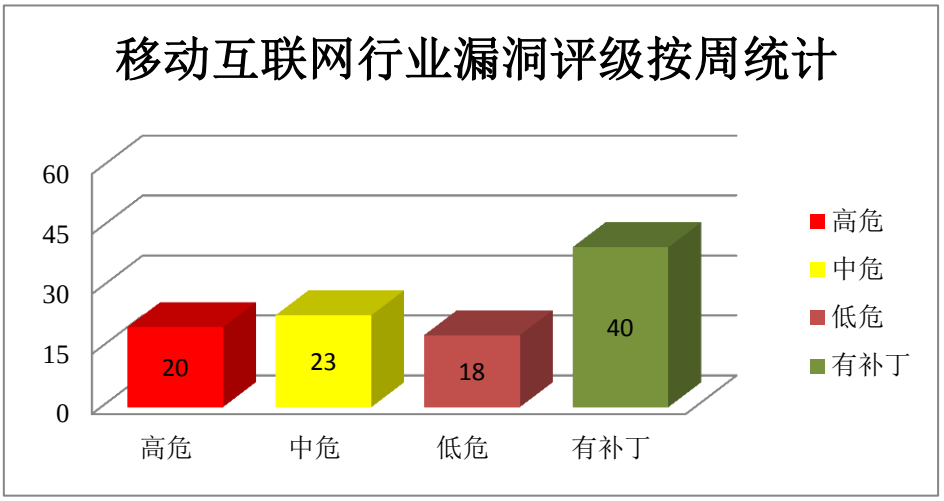

图 4 移动互联网行业漏洞统计

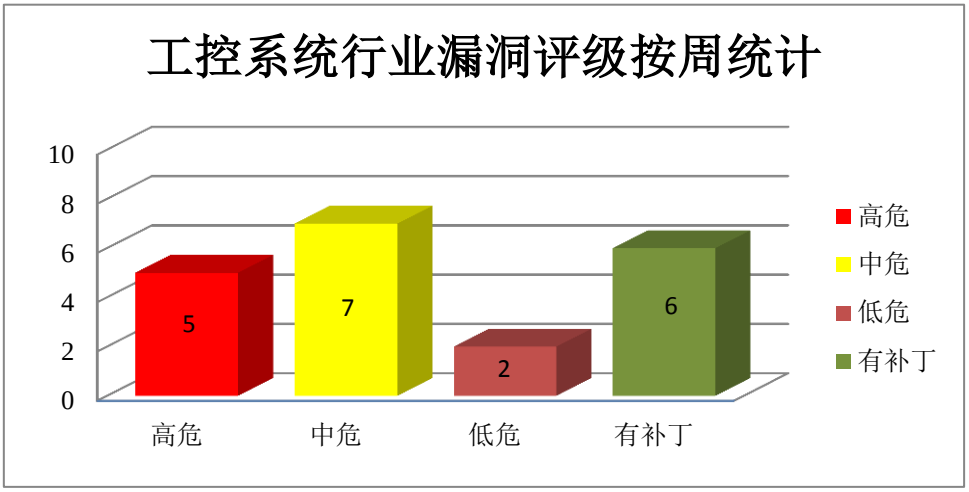

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

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。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Microsoft Windows 备份服务权限提升漏洞（CNVD-2020-56633、CNVD-2020-56636、CNVD-2020-56643）、Microsoft Windows 应用程序兼容性客户端库权限提升漏洞（CNVD-2020-56634、CNVD-2020-56637）、Microsoft Windows WER 权限提升漏洞、Microsoft Windows 备份服务权限提升漏洞、Microsoft Windows User Profile Service(ProfSvc)权限提升漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-56633

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56636

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56634

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56637

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56643

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56647

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56646

https://www.cnvd.org.cn/flaw/show/CNVD-2020-56645

2、Google 产品安全漏洞

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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 代码问题漏洞（CNVD-2020-55949、CNVD-2020-55948、CNVD-2020-55953、CNVD-2020-55952）、Google Android 信息泄露漏洞（CNVD-2020-55954）、Google Android 代码执行漏洞（CNVD-2020-55957）、Google Android 权限提升漏洞（CNVD-2020-55956、CNVD-2020-56129）。其中，除“Google Android 信息泄露漏洞（CNVD-2020-55954）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-55949
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55948
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55954
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55953
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55952
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55957
https://www.cnvd.org.cn/flaw/show/CNVD-2020-55956
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56129

3、IBM 产品安全漏洞

IBM Informix Dynamic Server（IDS）是一款可扩展的对象关系数据库服务器，它为集群数据中心提供持续数据可用性和灾难恢复等功能。IBM Curam Social Program Management 是一套社会计划管理解决方案，支持端到端社会项目交付流程。IBM Maximo Asset Management 是一个针对资产密集型行业的综合解决方案，用于通过公共平台管理企业实物资产。IBM Security Access Manager 是一款简单的访问管理解决方案，可帮助企业防范威胁漏洞。IBM Cognos Analytics 是一套商业智能软件，可提供有价值的信息、安全的数据治理和报告。IBM InfoSphere Information Server 是一套数据整合平台，包含一系列产品，使您能够理解、清理、监控、转换及传送数据，以及协作以弥合业务与 IT 之间的差距。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过认证，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Security Guardium 信息泄露漏洞（CNVD-2020-56393）、IBM InfoSphere Information Server HTML 注入漏洞、IBM Security Guardium CSV 注入漏洞、IBM Informix Dynamic Server 授权问题漏洞、IBM Curam Social Program Management 跨站请求伪造漏洞（CNVD-2020-56450）、IBM Maximo Asset Management 认证绕过漏洞、IBM Security Access Manager 跨站脚本漏洞（CNVD-2020-56453）、IBM Cognos Analytics CSV 注入漏洞。其中，“IBM Security Guardium CSV 注入漏洞、IBM Curam Social Program Management 跨站请求伪造漏洞（CNVD-2020-

56450）、IBM Maximo Asset Management 认证绕过漏洞、IBM Cognos Analytics CSV 注入漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-56393
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56398
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56397
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56402
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56450
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56449
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56453
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56451

4、Cisco 产品安全漏洞

Cisco StarOS 是一套路由器操作系统，可控制整个系统逻辑，可控制进程和 CLI。Cisco IOS XE 是美国 Cisco 公司为其网络设备开发的一套基于 Linux 内核的模块化操作系统。Cisco FXOS 是 Firepower 可扩展操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco StarOS 权限提升漏洞（CNVD-2020-56458、CNVD-2020-56463）、Cisco IOS XE 拒绝服务漏洞（CNVD-2020-56462、CNVD-2020-56629）、Cisco IOS XE 命令注入漏洞（CNVD-2020-56465）、Cisco FXOS 缓冲区溢出漏洞、Cisco IOS XE Software 任意代码执行漏洞、Cisco IOS XE 任意代码执行漏洞（CNVD-2020-56468）。其中，除“Cisco StarOS 权限提升漏洞（CNVD-2020-56458）\Cisco IOS XE 拒绝服务漏洞（CNVD-2020-56462）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-56458
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56462
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56465
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56463
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56467
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56466
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56468
https://www.cnvd.org.cn/flaw/show/CNVD-2020-56629

5、GitLab 跨站脚本漏洞（CNVD-2020-56448）

GitLab 是一个利用 Ruby on Rails 开发的开源应用程序，实现一个自托管的 Git 项目仓库，可通过 Web 界面进行访问公开的或者私人项目。本周，GitLab 被披露存在跨

站脚本漏洞。攻击者可通过组名称利用该漏洞进行跨站脚本攻击。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-56448

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2020-55743	Oracle Fusion Middleware Coherence 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.oracle.com/security-alerts/cpujul2020.html
CNVD-2020-55745	Linux kernel 资源管理错误漏洞（CNVD-2020-55745）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.kernel.org/
CNVD-2020-55776	MyBatis 远程代码执行漏洞	高	MyBatis 3.5.6 版本已修复此漏洞，建议用户下载使用：https://github.com/mybatis/mybatis-3/pull/2079
CNVD-2020-56118	LAquis SCADA 越界读取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://laquisscada.com/
CNVD-2020-56124	MOXA NPort IAW5000A-I/O Series 会话固定漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.moxa.com/en/support/product-support/software-and-documentation/search?psid=50535
CNVD-2020-56642	Microsoft Windows TCP/IP 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
CNVD-2020-56729	SonicOS 缓冲区溢出漏洞（CNVD-2020-56729）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0008
CNVD-2020-57048	AVEVA eDNA Enterprise Data Historian SQL 注入漏洞（CNVD-2020-57048）	高	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.aveva.com/
CNVD-2020-57067	GitLab 访问控制问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://gitlab.com/gitlab-org/cves/-/blob/

			master/2020/CVE-2020-13296.json
CNVD-2020-57110	libarchive 堆缓冲区溢出漏洞（CNVD-2020-57110）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/libarchive/libarchive/commit/4f085eea879e2be745f4d9bf57e8513ae48157f4

小结：本周，Microsoft 产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，Google、IBM、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过认证，获取敏感信息，提升权限，执行任意代码，导致拒绝服务等。另外，GitLab 被披露存在跨站脚本漏洞。攻击者可通过组名称利用该漏洞进行跨站脚本攻击。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、WordPress Colorbox Lightbox 跨站脚本漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress Colorbox Lightbox 存在跨站脚本漏洞。攻击者可利用漏洞在受影响站点的上下文中执行任意脚本代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/158882/WordPress-Colorbox-Lightbox-1.1.2-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-57116

信息提供者

深信服科技股份有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Linux 内核曝严重蓝牙漏洞，影响多个版本

谷歌安全研究人员在 Linux Kernel 中发现了一组蓝牙漏洞（BleedingTooth），该漏洞可能允许攻击者进行零点击攻击，运行任意代码或访问敏感信息。

BleedingTooth 漏洞分别被命名为 CVE-2020-12351，CVE-2020-12352 和 CVE-2020-24490。其中最严重的漏洞是基于堆的类型混淆漏洞（CVE-2020-12351），被评为高危漏洞，CVSS 评分达到 8.3。据悉，漏洞存在于 BlueZ 中，软件栈默认情况下为 Linux 实现了所有蓝牙核心协议和层。除 Linux 笔记本电脑外，它还用于许多消费或工业物联网设备。受害者蓝牙覆盖范围内的远程攻击者都可以通过目标设备的 bd 地址来利用此漏洞。攻击者能够通过发送恶意的 l2cap 数据包来触发漏洞，导致拒绝服务，甚至执行具有内核特权的任意代码。

参考链接：https://www.freebuf.com/news/252048.html

2. Adobe 解决了 Adobe Flash Player 中的一个严重安全漏洞

Adobe 发布了安全更新，旨在解决 Adobe Flash Player 中一个严重的远程代码执行漏洞。攻击者可以在不知道用户访问网站的情况下简单地在 HTTP 响应中插入恶意字符串，并利用此漏洞。

参考链接：https://securityaffairs.co/wordpress/109448/hacking/adobe-flash-player-critical-flaw.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537