国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 12 月 07 日-2020 年 12 月 13 日　　2020 年第 50 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 293 个，其中高危漏洞 142 个、中危漏洞 134 个、低危漏洞 17 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 67%），其中互联网上出现“Wordpress Theme Wibar 'Brand Component'跨站脚本漏洞、WordPress 插件 Heroic Knowledge Base 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 12235 个，与上周（6960 个）环比增加 76%。

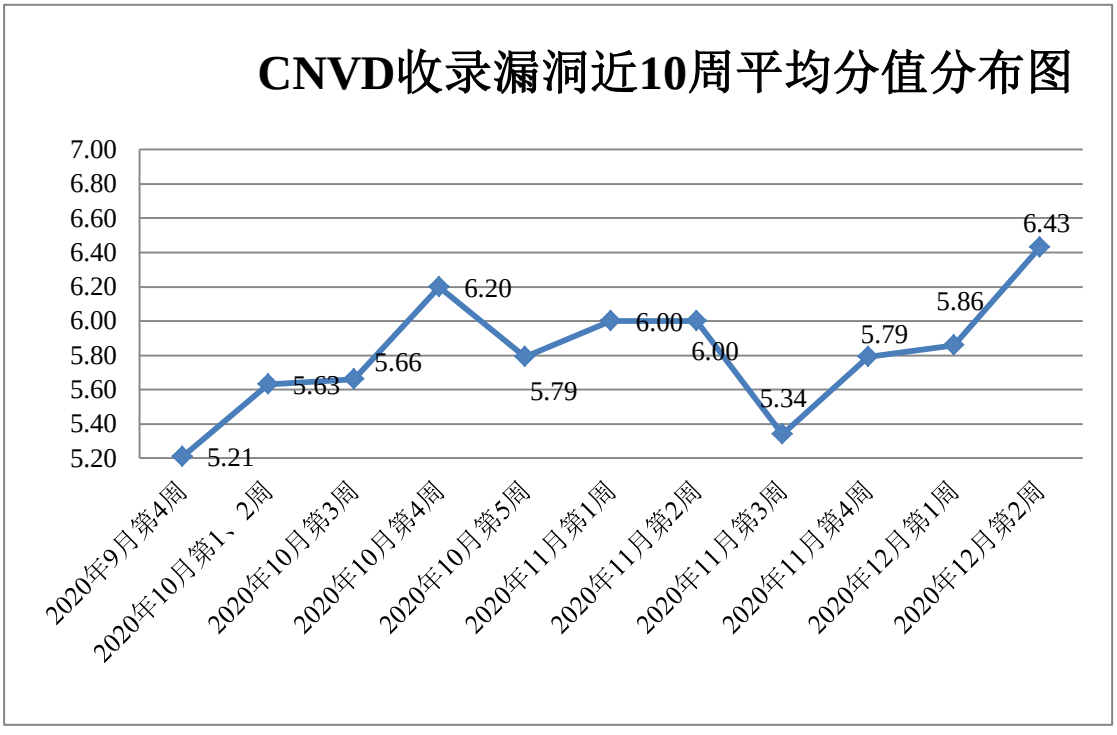

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 18 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 570 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 56 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 22 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：

广州科密智能科技有限公司、上海穆云智能科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京易成时代科技有限公司、北京数字政通科技股份有限公司、华硕电脑股份有限公司、北京火绒网络科技有限公司、远齐科技（北京）有限公司、重庆楚捷科技有限公司、杭州游卡网络技术有限公司、北京网易有道计算机系统有限公司、北京爱奇艺科技有限公司、随锐科技集团股份有限公司、中移铁通有限公司智能产品分公司、厦门昕桐科技有限公司、北京猿力教育科技有限公司、广州网易计算机系统有限公司、钉钉（中国）信息技术有限公司、深圳市河辰通讯技术有限公司、广州华多网络科技有限公司、数德科技（北京）有限公司、网易有道信息技术（北京）有限公司、武汉斗鱼网络科技有限公司、鹏为软件股份有限公司、东莞市智跃软件科技有限公司、北京网景盛世技术开发中心、南京九则软件科技有限公司、山东义理信息技术有限公司、新开普电子股份有限公司、艾科瑞（北京）仪器仪表有限公司、北京普艾斯科技有限公司、上海衿领信息科技有限公司、浙江淘宝网络有限公司、深圳市网旭科技有限公司、南京千知寻网络科技有限公司、优酷信息技术（北京）有限公司、上海赛连信息科技有限公司、上海喜马拉雅科技有限公司、北京金山办公软件股份有限公司、北京印象笔记科技有限公司、上海楚果信息技术有限公司、北京山石网科信息技术有限公司、网伦天下（北京）智能科技有限公司、西门子（中国）有限公司、北京通达信科科技有限公司、深圳市迅雷网络技术有限公司、济南亘安信息技术有限公司、沈阳云创未来科技有限公司、金山软件股份有限公司、深圳立讯检测股份有限公司、山西龙采科技有限公司运城分公司、猎豹移动公司、湖南快乐阳光互动娱乐传媒有限公司、苹果电子产品商贸（北京）有限公司、邢台市网商软件开发有限公司、武汉贝云网络科技有限公司、北京中成科信科技发展有限公司、慈溪市友诚网络科技有限公司、北京酷我科技有限公司、广东凯格科技有限公司、北京奥博威斯科技有限公司、微软(中国)有限公司、武汉思创易控科技有限公、北京华信傲天网络技术有限公司、哈尔滨伟成科技有限公司、阿尔卡特朗讯（中国）投资有限公司、上海荃路软件开发工作室、信呼、施耐德（Schneider Electric）、米酷资源网、UCMS、vaeThink、pig 和 SeaCMS。

本周，CNVD 发布了《Microsoft 发布 2020 年 12 月安全更新》、《关于 Apache Struts2 存在远程代码执行漏洞（S2-061）的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5896

https://www.cnvd.org.cn/webinfo/show/5899

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、厦门服云信息科技有限公司、深信服科技股份有限公司、华为技术有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、国瑞数码零点实验室、北京天地和兴科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、新疆海狼科技有限公司、山东华鲁科技发展股份有限公司、安徽长泰信息安全服务有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、河南灵创电子科技有限公司 、杭州海康威视数字技术股份有限公司、西门子（中国）有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、北京零零信安科技有限公司、南京众智维信息科技有限公司、广州市蓝爵计算机科技有限公司、北京华云安信息技术有限公司、上海观安信息技术股份有限公司、北京知道创宇信息技术股份有限公司、四川哨兵信息科技有限公司、广西等保安全测评有限公司、京东云安全、国家互联网应急中心、海南神州希望网络有限公司、北京机沃科技有限公司、北京智游网安科技有限公司、北京赛克艾威科技有限公司、雷石安全实验室、上海纽盾科技股份有限公司、武汉明嘉信信息安全检测评估有限公司、浙江安腾信息技术有限公司及其他个人白帽子向 CNVD 提交了 12235 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 10124 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）	6391	6391
斗象科技（漏洞盒子）	3259	3259
上海交大	474	474
哈尔滨安天科技集团股份有限公司	242	0
厦门服云信息科技有限公司	135	0
深信服科技股份有限公司	118	0
华为技术有限公司	94	0
新华三技术有限公司	82	0
北京数字观星科技有限公司	49	0
北京启明星辰信息安全技术有限公司	49	2
北京奇虎科技有限公司	47	15

北京天融信网络安全技术有限公司	44	3
中国电信股份有限公司网络安全产品运营中心	19	0
浙江大华技术股份有限公司	13	13
中国电信集团系统集成有限责任公司	2	2
北京神州绿盟科技有限公司	1	1
山东云天安全技术有限公司	332	332
国瑞数码零点实验室	119	119
北京天地和兴科技有限公司	115	115
远江盛邦（北京）网络安全科技股份有限公司	70	70
新疆海狼科技有限公司	61	61
山东华鲁科技发展股份有限公司	34	34
安徽长泰信息安全服务有限公司	27	27
北京云科安信科技有限公司（Seraph 安全实验室）	26	26
河南灵创电子科技有限公司	25	25
杭州海康威视数字技术股份有限公司	18	18
西门子（中国）有限公司	16	0
河南信安世纪科技有限公司	15	15
杭州迪普科技股份有限公司	14	0
北京零零信安科技有限公司	9	9
南京众智维信息科技有限公司	6	6
广州市蓝爵计算机科技有限公司	5	5
北京华云安信息技术有限公司	5	5
上海观安信息技术股份有限公司	5	5
北京知道创宇信息技术股份有限公司	5	0
四川哨兵信息科技有限公司	4	4
广西等保安全测评有限公司	3	3
京东云安全	3	3
国家互联网应急中心	3	3

海南神州希望网络有限公司	1	1
北京机沃科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京赛克艾威科技有限公司	1	1
雷石安全实验室	1	1
上海纽盾科技股份有限公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
浙江安腾信息技术有限公司	1	1
青海分中心	7	7
宁夏分中心	4	4
贵州分中心	1	1
四川分中心	1	1
浙江分中心	1	1
个人	1168	1168
报送总计	13129	12235

本周漏洞按类型和厂商统计

本周，CNVD 收录了 293 个漏洞。应用程序 129 个，WEB 应用 118 个，网络设备（交换机、路由器等网络端设备）18 个，数据库 9 个，智能设备（物联网终端设备）7 个，安全产品 7 个，操作系统 5 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	129
WEB 应用	118
网络设备（交换机、路由器等网络端设备）	18
数据库	9
智能设备（物联网终端设备）	7
安全产品	7
操作系统	5

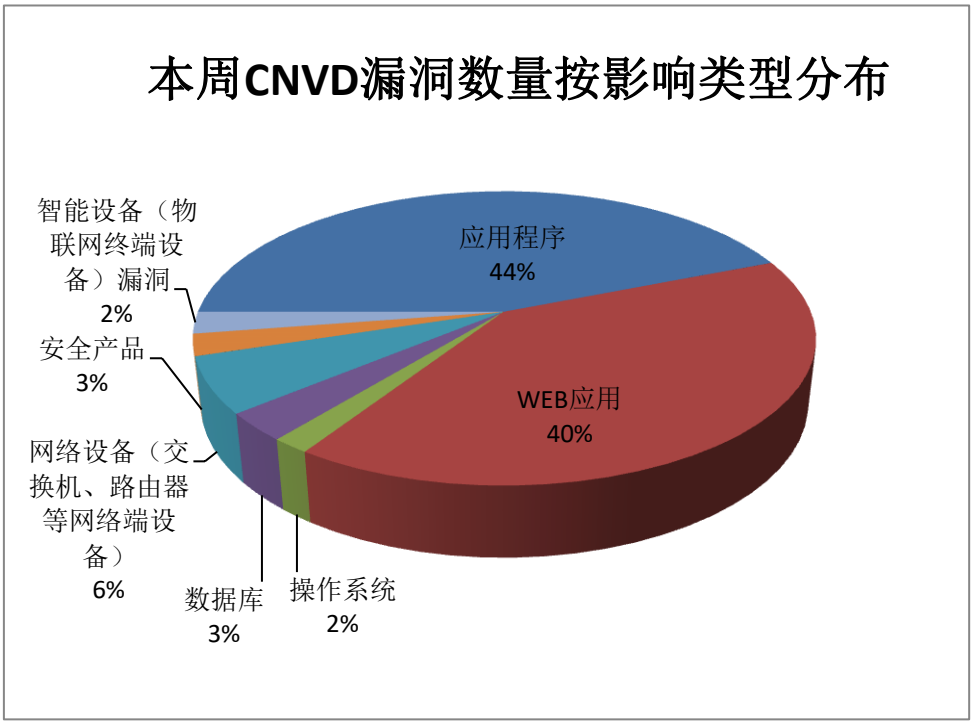

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、浙江浙大中控信息技术有限公司、Cisco 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	Siemens	18	6%
2	浙江浙大中控信息技术有限公司	15	5%
3	Cisco	13	4%
4	Oracle	13	4%
5	北京中成科信科技发展有限公司	10	3%
6	Schneider Electric	9	3%
7	CloudBees	7	3%
8	Crafter CMS	7	3%
9	WordPress	7	3%
10	其他	194	66%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，10 个移动互联网行业漏洞，34 个工控行业漏洞（如下图所示）。其中，“Cisco SD-WAN Software 权限提升漏洞、Cisco IP 电话

7800 系列和 8800 系列远程代码执行漏洞、SIEMENS SICAM A8000 RTUs SSL 配置不安全漏洞、Siemens XHQ 跨站脚本漏洞（CNVD-2020-70928）”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/

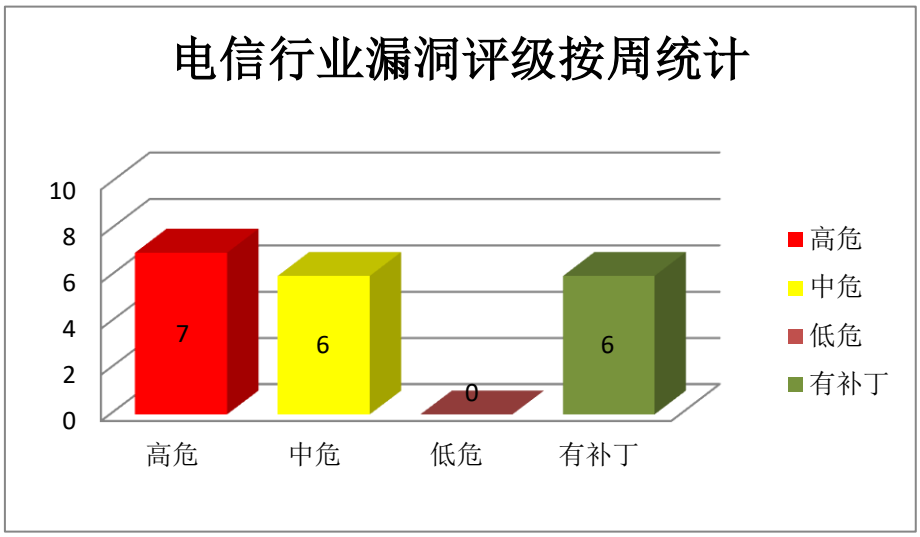

图 3 电信行业漏洞统计

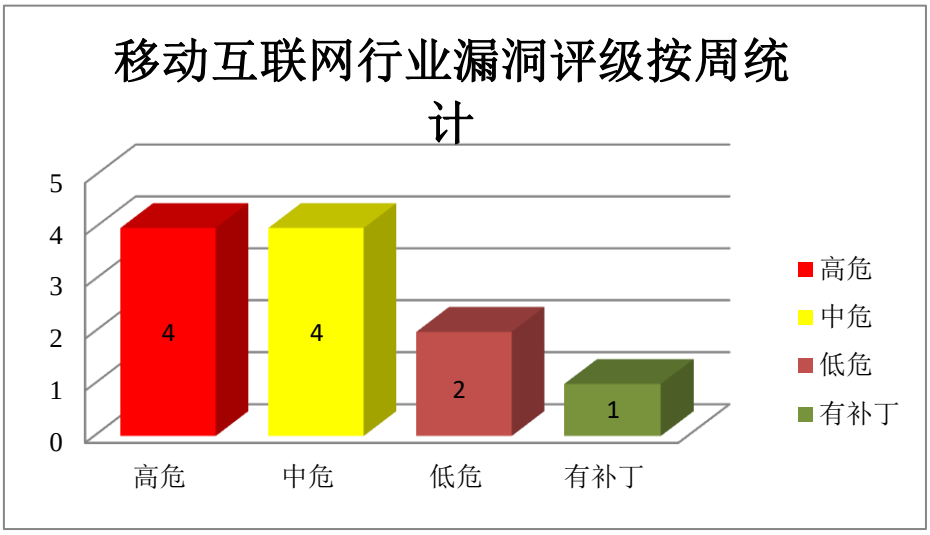

图 4 移动互联网行业漏洞统计

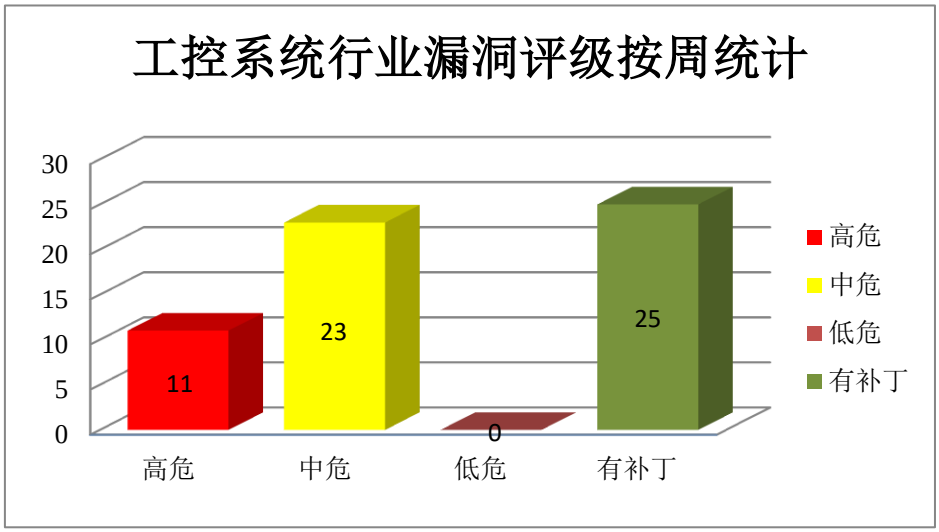

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens LOGO! 8 BM 是一个用于工业环境用于 Windows 平台的编程软件。Siemens XHQ 是一种软件平台，它汇集了工厂或管道运营数据，并对这些数据进行面向目标的处理，然后实时地做出决策，并有效提升工厂或管道运营绩效。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，进行跨站请求伪造攻击等。

CNVD 收录的相关漏洞包括：Siemens LOGO! 8 BM 授权问题漏洞、Siemens XHQ 跨站请求伪造漏洞（CNVD-2020-70927）、Siemens LOGO! 8 BM 信息泄露漏洞、Siemens XHQ SQL 注入漏洞、Siemens XHQ 跨站脚本漏洞（CNVD-2020-70928、CNVD-2020-70932、CNVD-2020-70931）、Siemens XHQ 信息泄露漏洞。其中，除“Siemens LOGO! 8 BM 授权问题漏洞、Siemens LOGO! 8 BM 信息泄露漏洞、Siemens XHQ 信息泄露漏洞”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-2020-70923

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70927

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70924

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70930

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70928

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70933

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70932

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70931

2、Oracle 产品安全漏洞

Oracle Universal Work Queue 是一种灵活的工作演示和访问工具。Oracle WebLogic Server 是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。Oracle Database Server 是一套关系数据库管理系统。Oracle MySQL 是一套开源的关系数据库管理系统。Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的机密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle Universal Work Queue 代码执行漏洞、Oracle WebLogic Server Console 远程代码执行漏洞、Oracle Database Server Vault component 未授权访问漏洞、Oracle MySQL Server 拒绝服务漏洞（CNVD-2020-70270）、Oracle Coherence 远程代码执行漏洞、Oracle Weblogic Server 信息泄露漏洞、Oracle WebCenter Sites 信息泄露漏洞、Oracle Access Manager 远程代码执行漏洞。其中，“Oracle Universal Work Queue 代码执行漏洞、Oracle WebLogic Server Console 远程代码执行漏洞、Oracle Coherence 远程代码执行漏洞”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-2020-70269
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70267
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70271
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70270
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70276
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70275
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70274
https://www.cnvd.org.cn/flaw/show/CNVD-2020-70273

3、Cisco 产品安全漏洞

Cisco SD-WAN vManage 是一款可提供软件定义网络功能的软件。Cisco Integrated Management Controller (IMC)是一个为 Cisco UCS C 系列机架式服务器和 Cisco S 系列存储服务器提供嵌入式服务器管理的基板管理控制器。Cisco Webex Teams 是一款综合通信应用程序，旨在为您提供所有必要的工具和合适的环境以增强团队协作。Cisco Firepower Management Center（FMC）是新一代防火墙管理中心软件。Cisco Firepower Threat Defense 是一款提供下一代防火墙服务的统一软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取系统文件，执行任意命令，获得 root 用户特权等。

CNVD 收录的相关漏洞包括：Cisco SD-WAN vManage 目录遍历漏洞、Cisco SD-WAN Software 权限提升漏洞、Cisco Integrated Management Controller 命令注入漏洞（C

NVD-2020-70859）、Cisco Integrated Management Controller 授权绕过漏洞、Cisco Webex Teams 跨站脚本漏洞、Cisco Firepower Management Center (FMC)跨站脚本漏洞、Cisco Firepower Threat Defense sfmgr 命令目录遍历漏洞、Cisco IOS 和 IOS XE 输入验证错误漏洞（CNVD-2020-70878）。其中，“Cisco SD-WAN Software 权限提升漏洞”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-2020-70854

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70852

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70859

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70858

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70855

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70861

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70860

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70878

4、Schneider Electric 产品安全漏洞

Schneider Electric Interactive Graphical SCADA System（IGSS）是一套用于监控和控制工业过程的 SCADA（数据采集与监控系统）系统。Schneider Electric EcoStruxure Building Operation Enterprise Server 是一个企业级楼宇控制系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得用户特权，远程执行代码。

CNVD 收录的相关漏洞包括：Schneider Electric Interactive Graphical SCADA System 缓冲区溢出漏洞（CNVD-2020-70522、CNVD-2020-70521、CNVD-2020-70525、CNVD-2020-70524、CNVD-2020-70523、CNVD-2020-70530）、Schneider Electric Interactive Graphical SCADA System 代码执行漏洞、Schneider Electric EcoStruxure Building Operation Enterprise Server 本地提权漏洞。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-2020-70522

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70521

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70525

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70524

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70523

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70529

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70530

https://www.cnvd.org.cn/flaw/show/CNVD-2020-70531

5、Huawei HedEx Lite (DM)路径遍历漏洞

Huawei HedEx Lite 是一款产品文档管理器。Huawei HedEx Lite (DM)被披露存在

路径遍历漏洞。攻击者可利用漏洞通过远程请求未经授权更改本地路径来请求本地文件或资源。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-2020-70940

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-2020-69833	Apache Struts 远程代码执行漏洞（CNVD-2020-69833）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cwiki.apache.org/confluence/display/WW/S2-061
CNVD-2020-70263	Cloudbees Jenkins Plugin Installation Manager Tool 存在未明漏洞	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.jenkins.io/security/advisory/2020-12-03/#SECURITY-1856
CNVD-2020-70276	Oracle Coherence 远程代码执行漏洞	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/cpuapr2020.html
CNVD-2020-70515	Crafter Studio 目录遍历漏洞（CNVD-2020-70515）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.craftercms.org/en/3.0/security/advisory.html
CNVD-2020-70852	Cisco SD-WAN Software 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vepescm-BjgQm4vJ
CNVD-2020-70926	SIEMENS SICAM A8000 RTUs SSL 配置不安全漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/pdf/ssa-415783.pdf
CNVD-2020-70950	Microsoft Windows Common Log File System Driver 权限许可和访问控制问题漏洞	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/zh-CN/security-guidance/advisory/CVE-2019-0959
CNVD-2020-70946	DPDK iv_data 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://launchpad.net/ubuntu/+source/dp

			dk/19.11.3-0ubuntu0.2?_ga=2.172564195.1337156165.1601345194-837715814.1599020068
CNVD-2020-70268	Oracle Trade Management 未授权访问漏洞	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/cpuoct2020.html
CNVD-2020-70927	Siemens XHQ 跨站请求伪造漏洞（CNVD-2020-70927）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://us-cert.cisa.gov/ics/advisories/icsa-20-343-06

小结：本周，Siemens 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，进行跨站请求伪造攻击等。此外，Oracle、Cisco、Schneider Electric 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取系统文件，执行任意命令，获得 root 用户特权等。另外，Huawei HedEx Lite (DM)被披露存在路径遍历漏洞。攻击者可利用漏洞通过远程请求未经授权更改本地路径来请求本地文件或资源。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 插件 Heroic Knowledge Base SQL 注入漏洞

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 插件 Heroic Knowledge Base 存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。

验证信息

POC 链接：https://packetstormsecurity.com/files/160279/WordPress-Heroic-Knowledge-Base-3.0.1-SQL-Injection.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-70943

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. 星巴克移动平台中发现了远程执行代码漏洞

星巴克的一个移动域中已修补了潜在的远程代码执行（RCE）错误。这家美国咖啡巨头在 HackerOne 上运行一个漏洞赏金平台。由 Kamil“ ko2sec” OnurÖzkaleli 提交的新漏洞报告于 11 月 5 日首次提交，并于 12 月 9 日公开。

参考链接：https://www.zdnet.com/article/remote-code-execution-vulnerability-uncovered-in-starbucks-mobile-platform/

2. 研究称通用电气医疗成像设备中的硬编码密码或使患者数据面临风险

根据安全公司 CyberMDX 的新发现，通用电气公司制造的数十种医疗成像设备都有硬编码的默认密码，这些密码不容易改变，但可能被利用来访问敏感的病人扫描数据。

参考链接：https://www.cnbeta.com/articles/tech/1063557.htm

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