国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 07 月 13 日-2020 年 07 月 19 日　　2020 年第 29 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 336 个，其中高危漏洞 133 个、中危漏洞 167 个、低危漏洞 36 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 146 个（占 43%），其中互联网上出现“Wordpress 插件 Powie's WHOIS Domain Check 存储型跨站脚本漏洞、Online Polling System 身份验证绕过 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 3700 个，与上周（4971 个）环比减少 26%。

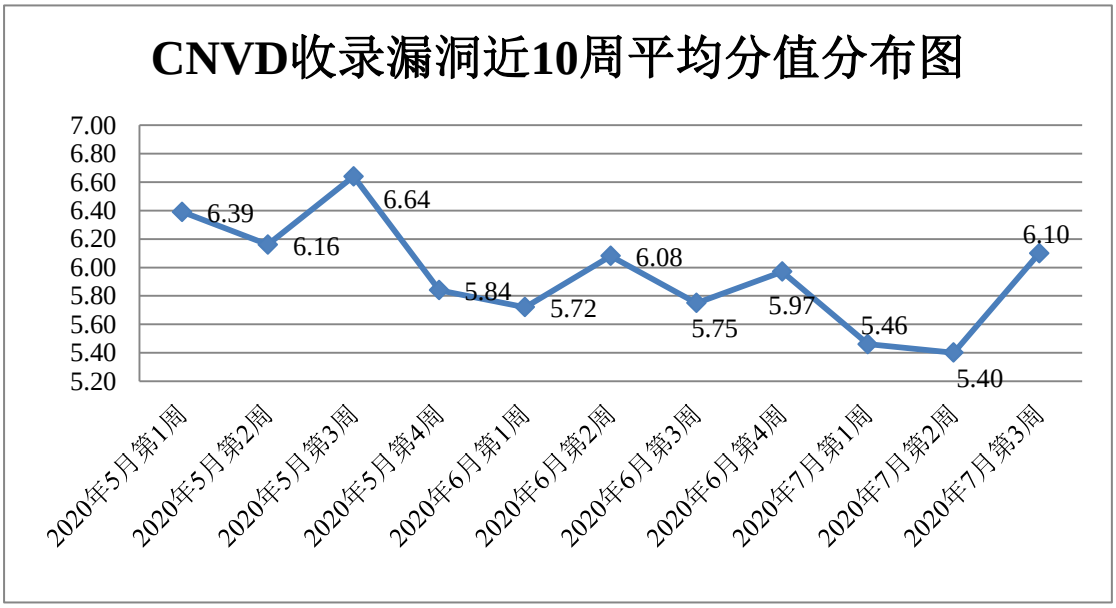

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 29 起，向基础电信企业通报漏洞事件 47 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 352 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 64 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 36 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：

中国电建集团贵阳勘测设计研究院有限公司、宜兴市兴晟信息科技有限公司、台安科技（无锡）有限公司、润申信息科技(上海)有限公司、上海孚盟软件有限公司、天津市集翔企商科技有限公司、上海明牛云科技有限公司、重庆巨泰物联网集团有限公司、江西金磊科技发展有限公司、心升时代(北京)科教仪器有限公司、铭飞科技有限公司、重庆匠果科技有限公司、海南大显科技有限公司、北京良精志诚科技有限责任公司、宜兴网络公司、ABB（中国）有限公司、温州乔宇科技有限公司、聊城市天际网络科技有限公司、石家庄百成网络科技有限公司、桂林崇胜网络科技有限公司、广州齐博网络科技有限公司、沧州佳蓝网络科技有限公司、景腾多媒體股份有限公司、北京网瑞达科技有限公司、研华科技（中国）有限公司、深圳市昂捷信息技术股份有限公司、济南速动信息科技有限公司、 宜兴易发网络服务有限公司、廊坊市极致网络科技有限公司、上海有品网络科技有限公司、山东城通科技有限公司、重庆远秋科技公司、无锡易商科技有限公司、成都飞鱼星科技股份有限公司、许昌永诚网络科技有限公司、北京通达志成科技有限公司、深圳市圆梦云科技有限公司、景德镇铭飞科技有限公司、上海麦克风文化传媒有限公司、上海安硕信息技术股份有限公司、长沙德尚网络科技有限公司、上海荃路软件开发工作室、深圳市锟铻科技有限公司、成都奥科睿科技有限公司、江下信息科技（惠州）有限公司、聊城市东昌府区天际网络科技有限公司、苏州科达科技股份有限公司、梅州市中业科技有限公司、常州遨翔网络科技有限公司、深圳锐取信息技术股份有限公司 、镇江市云优网络科技有限公司、青岛乾程控股集团有限公司、徐州金蝶软件有限公司、郑州狼烟网络科技有限公司、南昌卓蓝科技有限公司、淄博闪灵网络科技有限公司、中国国际航空股份有限公司、湖南翱云网络科技有限公司、海南易而优科技有限公司、海南赞赞网络科技有限公司、中国知网、网展科技、剑鱼论坛、飞飞影视导航系统、李雷博客、雷风影视、ZBlogger 社区、Heybbs、Jupyter、ZZCMS、YCCMS、Kkcms、Joomla!、Zzzcms 和 WIRIS。

本周，CNVD 发布了《关于 Windows DNS Server 存在远程代码执行漏洞的安全公告》、《Microsoft 发布 2020 年 7 月安全更新》、《Oracle 发布 2020 年 7 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5617

https://www.cnvd.org.cn/webinfo/show/5615

https://www.cnvd.org.cn/webinfo/show/5619

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、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、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、山东道普测评技术有限公司、北京云科安信科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、河南灵创电子科技有限公司、山东云天安全技术有限公司、长春嘉诚信息技术股份有限公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、广州市蓝爵计算机科技有限公司、山东华鲁科技发展股份有限公司、吉林谛听信息技术有限公司、泽鹿安全、北京禹宏信安科技有限公司、安徽长泰信息安全服务有限公司、浙江鹏信信息科技股份有限公司、成都安美勤信息技术股份有限公司、上海纽盾科技股份有限公司、星云博创科技有限公司、上海上讯信息技术股份有限公司、南方电网数字电网研究院有限公司、北京智游网安科技有限公司、北京赛克艾威科技有限公司及其他个人白帽子向 CNVD 提交了 3700 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 2757 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
斗象科技（漏洞盒子）	1452	1452
奇安信网神（补天平台）	1001	1001
阿里云计算有限公司	999	0
哈尔滨安天科技集团股份有限公司	425	0
华为技术有限公司	307	0
上海交大	304	304
北京天融信网络安全技术有限公司	189	18
深信服科技股份有限公司	114	0
北京神州绿盟科技有限公司	91	1
北京启明星辰信息安全技术有限公司	76	13
新华三技术有限公司	44	0
北京奇虎科技有限公司	11	0

北京知道创宇信息技术股份有限公司	5	0
杭州安恒信息技术股份有限公司	1	1
国瑞数码零点实验室	252	252
山东道普测评技术有限公司	98	98
北京云科安信科技有限公司	64	64
远江盛邦（北京）网络安全科技股份有限公司	40	40
西门子（中国）有限公司	27	0
河南灵创电子科技有限公司	24	24
山东云天安全技术有限公司	14	14
杭州迪普科技股份有限公司	12	0
长春嘉诚信息技术股份有限公司	9	9
北京天地和兴科技有限公司	8	8
河南信安世纪科技有限公司	7	7
广州市蓝爵计算机科技有限公司	7	7
山东华鲁科技发展股份有限公司	7	7
吉林谛听信息技术有限公司	7	7
泽鹿安全	6	6
北京禹宏信安科技有限公司	4	4
安徽长泰信息安全服务有限公司	3	3
浙江鹏信信息科技股份有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
上海纽盾科技股份有限公司	2	2

星云博创科技有限公司	2	2
上海上讯信息技术股份有限公司	2	2
南方电网数字电网研究院有限公司	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
CNCERT 吉林分中心	1	1
CNCERT 云南分中心	1	1
个人	345	345
报送总计	5968	3700

本周漏洞按类型和厂商统计

本周，CNVD 收录了 336 个漏洞。应用程序 130 个，WEB 应用 115 个，操作系统 62 个，网络设备（交换机、路由器等网络端设备）23 个，智能设备（物联网终端设备）4 个，安全产品 1 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	130
WEB 应用	115
操作系统	62
网络设备（交换机、路由器等网络端设备）	23
智能设备（物联网终端设备）	4
安全产品	1
数据库	1

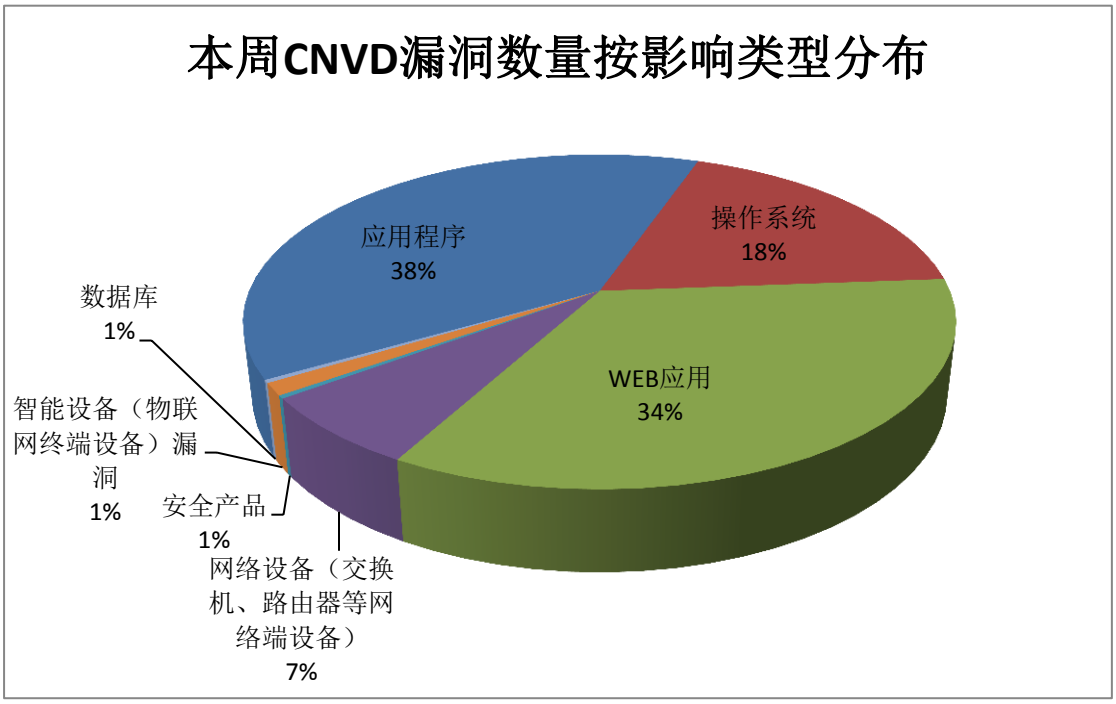

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Oracle、Rockwell Automation 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	38	11%
2	Oracle	32	9%
3	Rockwell Automation	19	5%
4	Siemens	15	4%
5	SAP	10	3%
6	FreeBSD	10	3%
7	Microsoft	9	2%
8	茉柏枘（上海）软件科技有限公司	9	2%
9	河南跃龙门科技有限公司	7	2%
10	其他	217	59%

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，47 个移动互联网行业漏洞，42 个工控行业漏洞（如下图所示）。其中，“多款 Rockwell Automation 产品路径遍历漏洞、Grundf

os CIM 500 访问控制错误漏洞、Samsung 移动设备缓冲区溢出漏洞（CNVD-2020-40834）、Oracle WebLogic Server 远程代码执行漏洞（CNVD-2020-38880）”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/

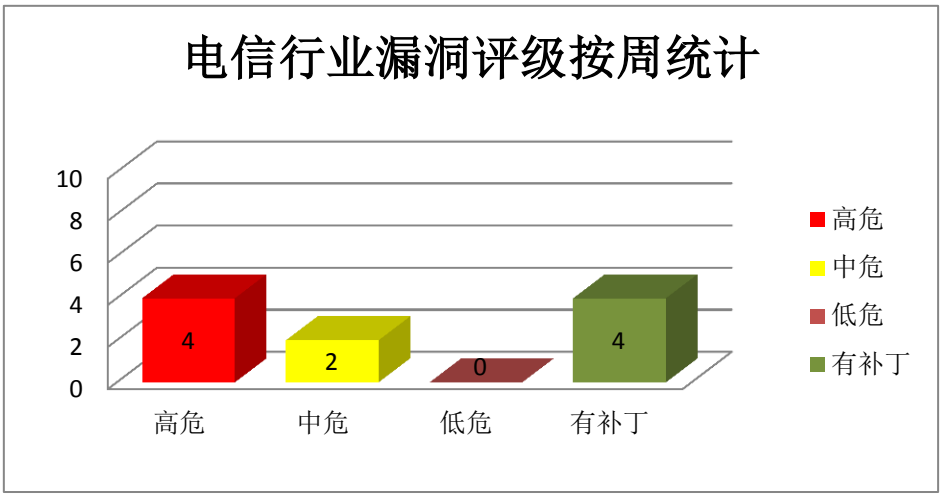

图 3 电信行业漏洞统计

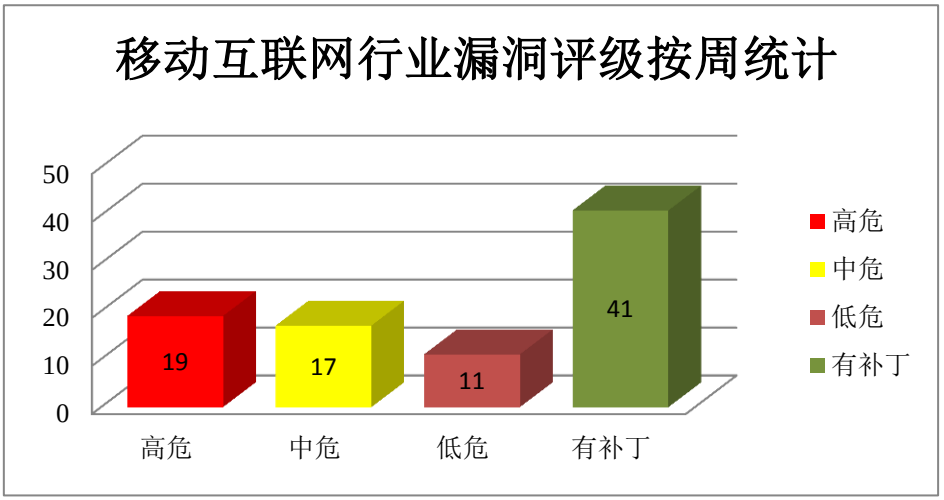

图 4 移动互联网行业漏洞统计

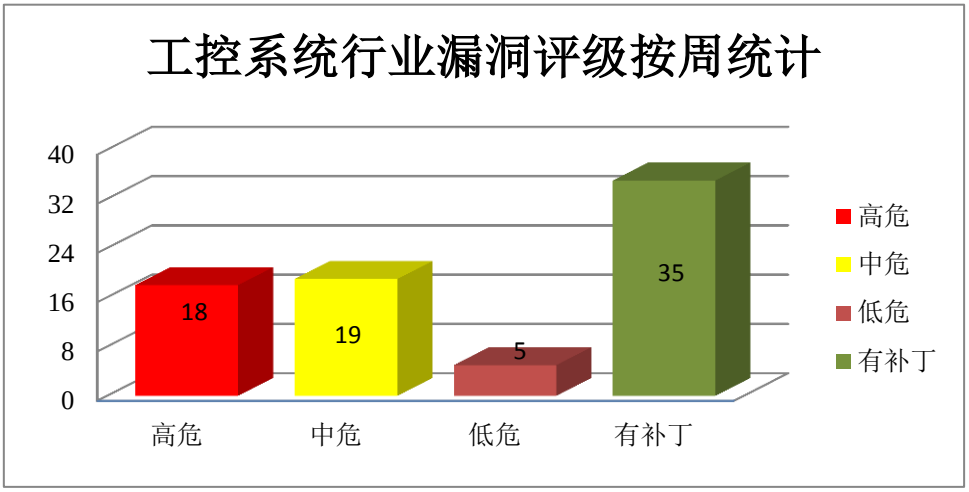

图 5 工控系统行业漏洞统计

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、 Rockwell Automation 产品安全漏洞

Rockwell Automation FactoryTalk Services Platform 是一套由多个产品组成的服务平台，它为应用程序提供常规服务，如诊断信息、健康监视和实时数据访问等。Rockwell Automation FactoryTalk View SE 是一款工业自动化系统视图界面。Rockwell Automation RSLinx Classic 是一套工业通信解决方案。Rockwell Automation FactoryTalk Linx 是一套工业通信解决方案。Rockwell Automation ControlFLASH 是一款固件更新实用程序。Rockwell Automation MicroLogix 1400 Controllers Series A 等都是美国罗克韦尔（Rockwell Automation）公司的可编程逻辑控制器。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，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Rockwell Automation FactoryTalk Services Platform XML 外部实体注入漏洞、Rockwell Automation FactoryTalk View SE 信息泄露漏洞（CNVD-2020-38417）、Rockwell Automation FactoryTalk View SE 权限许可和访问控制问题漏洞、多款 Rockwell Automation 产品路径遍历漏洞、多款 Rockwell Automation 产品代码问题漏洞、多款 Rockwell Automation 产品输入验证错误漏洞（CNVD-2020-38695）、Rockwell Automation FactoryTalk Services Platform 堆缓冲区溢出漏洞、多款 Rockwell Automation 产品拒绝服务漏洞。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-2020-38418

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38417

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38689

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38694

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38693

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38695

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38701

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38702

2、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。Microsoft .NET Core 是一套免费的开源开发平台。Microsoft .NET Framework 是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。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。Microsoft ASP .NET Core 是一框跨平台开源框架。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，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Windows Server DNS Server 远程代码执行漏洞、Microsoft Windows Kernel 提权漏洞（CNVD-2020-40625）、Microsoft .NET Core 和.NET Framework 拒绝服务漏洞、Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞（CNVD-2020-40627）、Microsoft ASP.NET Core 输入验证错误漏洞、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2020-40630）、Microsoft Windows GDI 信息泄露漏洞（CNVD-2020-40629）、Microsoft Windows Media Foundation 缓冲区溢出漏洞（CNVD-2020-40631。其中，“Microsoft Windows Server DNS Server 远程代码执行漏洞、Microsoft Windows Kernel 提权漏洞（CNVD-2020-40625）、Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞（CNVD-2020-40627）、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2020-40630）”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-2020-40487

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40625

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40628

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40627

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40626

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40630

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40629

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40631

3、SAP 产品安全漏洞

SAP Netweaver 是一套面向服务的集成化应用平台。SAP NetWeaver Application Server（AS）Java 是一款运行于 NetWeaver 中且基于 Java 编程语言的应用服务器。SAP Disclosure Management 是一套自动化财务披露管理系统。SAP Business Objects Business Intelligence Platform 是一套商业智能软件和企业绩效解决方案套件。SAP Fiori 是一套为 SAP 应用程序提供用户体验（UX）的设计系统，它为设计人员和开发人员提供了一套工具和指南，能够快速地开发适用于任何平台的应用，为创建者和用户提供一致、创新的体验。SAP Commerce 是一套基于云的电子商务平台。SAP NetWeaver AS ABAP Business Server 是一款适用于 ABAP（高级商务应用编程）的应用服务器。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞登录控制系统，获取敏感信息，将用户重定向到恶意的网站，执行客户端代码等。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS Java 命令执行漏洞、SAP Solution Manager 注入漏洞、SAP Disclosure Management 代码问题漏洞（CNVD-2020-40777、CNVD-2020-40778）、SAP Business Objects Business Intelligence Platform 信息泄露漏洞（CNVD-2020-40814）、SAP Fiori 输入验证错误漏洞、SAP Commerce 信息泄露漏洞、SAP NetWeaver AS ABAP Business Server 跨站脚本漏洞。其中，“SAP NetWeaver AS Java 命令执行漏洞”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-2020-38866

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40764

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40777

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40778

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40814

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40813

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40812

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40811

4、Siemens 产品安全漏洞

Siemens SIMATIC S7-200 Smart 是一款应用于中小型自动化系统中的可编程逻辑控制器（PLC）。Siemens LOGO!8 BM 是一款可编程逻辑控制器。Opcenter Execution Core（以前称为 Camstar Enterprise Platform）是一种通用的制造执行系统（MES）。SICAM T 是一种数字测量传感器，允许在单个单元中测量非电气网络中的电量。ICAM-MMU(Measurement and Monitoring Unit) 是一种功率监测装置，它允许在一个单元中

测量电网中的电量。SICAM SGU（已停产）是一种智能电网远程终端设备，具有电力公司和公用事业公司的通信能力。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数据库敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Siemens Opcenter Execution Core SQL 注入漏洞、Siemens Opcenter Execution Core 访问控制错误漏洞、Siemens SIMATIC S7-200 Smart CPU 系列拒绝服务漏洞、Siemens LOGO! 8 BM 缓冲区溢出漏洞、Siemens SICAM MMU、SGU 和 T 身份验证绕过漏洞、Siemens SICAM MMU、SGU 和 T 缓冲区溢出漏洞、Siemens SICAM MMU、SGU 和 T 跨站脚本漏洞（CNVD-2020-40616）、Siemens SICAM MMU、SGU 和 T 越界读取漏洞。其中，“Siemens SIMATIC S7-200 Smart CPU 系列拒绝服务漏洞、Siemens LOGO! 8 BM 缓冲区溢出漏洞、Siemens SICAM MMU、SGU 和 T 缓冲区溢出漏洞”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-2020-40862
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40861
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40865
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40864
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40614
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40617
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40616
https://www.cnvd.org.cn/flaw/show/CNVD-2020-40622

5、Phoenix Contact PC Worx 和 Worx Express 缓冲区溢出漏洞

Phoenix Contact PC Worx 和 Phoenix Contact PC Worx Express 都是德国菲尼克斯电气（Phoenix Contact）公司的一套用于 PLC（可编程逻辑控制器）的编程软件。本周，Phoenix Contact PC Worx 和 PC Worx Express 被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞执行代码。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-2020-38415

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-2020-38218	rConfig SQL 注入漏洞（CNVD-2020-38218）	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.rconfig.com/
CNVD-2020-	AnyDesk 格式化字符串错误	高	目前厂商已发布升级补丁以修复漏

38774	漏洞		洞，补丁获取链接：https://download.anydesk.com/changelog.txt
CNVD-2020-38778	FreeBSD 权限许可和访问控制问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.freebsd.org/advisories/FreeBSD-SA-19:11.cd_ioctl.asc
CNVD-2020-38866	SAP NetWeaver AS Java 命令执行漏洞	高	建议将 SAP 对应产品升级至安全版本，建议用户下载使用：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675
CNVD-2020-38877	Oracle WebLogic Server 远程代码执行漏洞（CNVD-2020-38877）	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://www.oracle.com/security-alerts/cpujul2020.html
CNVD-2020-38894	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2020-38894）	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.mozilla.org/en-US/security/advisories/mfsa2020-16/
CNVD-2020-40487	Microsoft Windows Server DNS Server 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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1350
CNVD-2020-40627	Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞（CNVD-2020-40627）	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-2020-1058
CNVD-2020-40736	OpenConnect 缓冲区溢出漏洞	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/openconnect/openconnect/-/merge_requests/108
CNVD-2020-40807	WordPress CodePeople Payment Form for PayPal Pro SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/payment-form-for-paypal-pro/#developers

小结：本周，Rockwell Automation 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，执行任意代码，发起拒绝服务攻击等。此外，Microsoft、SAP、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞登录控制系统，获取敏感信息，提升权限，将用户重定向到恶意的网站，执行任意代码，造成拒绝服务等。另外，Phoenix Contact PC Worx 和 PC Worx Express 被披露存在缓冲区溢出漏洞。远程攻击者可利用该

漏洞执行代码。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 Powie's WHOIS Domain Check 存储型跨站脚本漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

Wordpress 插件 Powie's WHOIS Domain Check 存在存储型跨站脚本漏洞。攻击者可以利用漏洞提升权限或执行管理员能够执行的任何操作。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35832

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-40623

信息提供者

CNVD 工作组

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. Windows DNS 服务器曝"蠕虫级"漏洞，已存在长达 17 年

研究人员新发现一个高度严重的可蠕虫漏洞 SigRed ，CVSS 评分为满分 10 分。该漏洞影响 2003 年-2019 年的 Windows Server 版本。SigRed 漏洞的高危害性在于其是可蠕虫的，也就是可以自传播的，无需用户交互就能传播到易受攻击的设备上，允许未经身份验证的远程攻击者获得针对目标服务器的域管理员特权，并完全控制组织的 IT 基础架构。

参考链接：https://www.freebuf.com/news/243542.html

2. Cisco 修复可致路由器被控制的超危 Pre-Auth 漏洞

7 月 15 日，Cisco 发布安全更新，修复超危远程代码执行，身份认证绕过和静态默认凭据漏洞，这些漏洞影响多款路由器和防火墙设备，可导致设备被攻击者完全控制。Cisco 还发布了一则安全更新，修复 Cisco Prime License Manager 软件中的一个权限提升漏洞。根据该公司的说法，目前没有变通措施可以用于修复这些漏洞。Cisco 将 15 日修复的五个安全漏洞的 CVSS 基础评分都评为 9.8，所以这五个漏洞都是超危漏洞。

参考链接：https://www.freebuf.com/vuls/243563.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