

信息安全漏洞周报

2020年08月31日-2020年09月06日

2020年第36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 465 个，其中高危漏洞 131 个、中危漏洞 274 个、低危漏洞 60 个。漏洞平均分为 5.73。本周收录的漏洞中，涉及 0day 漏洞 77 个（占 17%），其中互联网上出现“WordPress Vanguard 跨站脚本漏洞、Metasploit Framework 相对路径遍历漏洞”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 3165 个，与上周（4604 个）环比减少 45%。

CNVD收录漏洞近10周平均分分布图

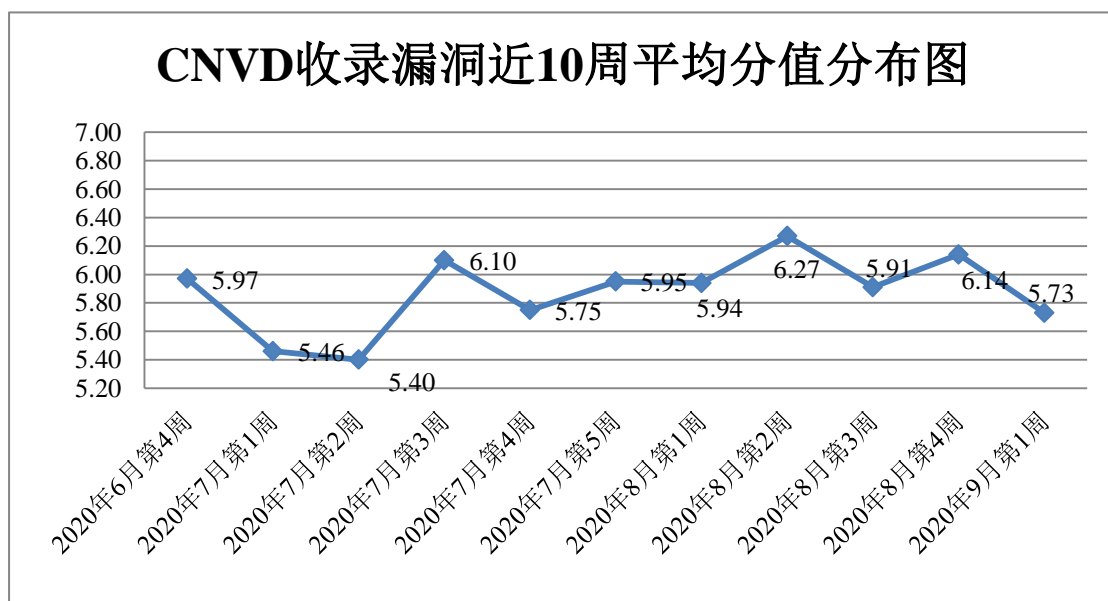


图 1 CNVD 收录漏洞近 10 周平均分分布图


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 20 起，向基础电信企业通报漏洞事件 6 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 211 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 50 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 23 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：

天津市集翔企商科技有限公司、北京融智创想信息技术有限公司、深圳市邦明科技有限公司、北京千真市场营销策划有限公司、联奕科技有限公司、中凯信息网络有限公司、青岛东胜伟业软件有限公司、杭州凡龙科技有限公司、中兴保全股份有限公司、郑州狼烟网络科技有限公司、无锡易商科技有限公司、北京通达志成科技有限公司、正方软件股份有限公司、深圳市大江网科技有限公司、中山市凝聚网络科技有限公司、无锡铭品网络科技有限公司、天津企朋科技发展有限公司、上海新浩艺软件有限公司、深圳市硕赢互动信息技术有限公司、温州乔宇科技有限公司、广州市竣达智能软件技术有限公司、北京超图软件股份有限公司、北京中创视讯科技有限公司、北京正影网络科技有限公司、珠海金山办公软件有限公司、河南利梭互联网信息技术有限公司、湖南翱云网络科技有限公司、北京五指互联科技有限公司、北京四方继保自动化股份有限公司、北京中庆纳博信息技术有限公司、山西牛酷信息科技有限公司、上海物创信息科技有限公司、广州合优网络科技有限公司、四平市九州易通科技有限公司、上海卓岚信息科技有限公司、太原迅易科技有限公司、北京中控科技发展有限公司、微软(中国)有限公司、研华科技(中国)有限公司、北京中庆现代技术股份有限公司、浙江齐治科技股份有限公司、沈阳点动科技有限公司、正光网络、李雷博客、狂雨小说 cms、UCMS、Delta Electronics 和 VMware, Inc.。



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、北京神州绿盟科技有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、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。国瑞数码零点实验室、山东华鲁科技发展股份有限公司、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、河南信安世纪科技有限公司、北京云科安信科技有限公司(Seraph 安全实验室)、北京华云安信息技术有限公司、山东云天安全技术有限公司、内蒙古奥创科技有限公司、南京众智维信息科技有限公司、杭州海康威视数字技术股份有限公司、北京顶象技术有限公司、山东道普测评技术有限公司、吉林谛听信息技术有限公司、北京天地和兴科技有限公司、安徽长泰信息安全服务有限公司、杭州迪普科技股份有限公司、广西等保安全测评有限公司、平安银河实验室、上海纽盾科技股份有限公司、上海观安信息技术股份有限公司、上海犀点意象网络科技有限公司、中科华威(北京)信息技术研究院、北京长亭科技有限公司、京东云安全、浙江安腾信息技术有限公司、北京智游网安科技有

限公司、北京惠而特科技有限公司、北京卓识网安技术股份有限公司、北京安华金和科技有限公司及其他个人白帽子向 CNVD 提交了 3165 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 2204 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）	1210	1210
上海交大	569	569
奇安信网神（补天平台）	425	425
哈尔滨安天科技集团股份有限公司	205	0
北京神州绿盟科技有限公司	163	9
华为技术有限公司	128	0
北京天融信网络安全技术有限公司	117	19
新华三技术有限公司	114	0
深信服科技股份有限公司	94	1
北京启明星辰信息安全技术有限公司	57	11
北京数字观星科技有限公司	24	0
北京知道创宇信息技术股份有限公司	14	0
恒安嘉新(北京)科技股份有限公司	9	0
北京安信天行科技有限公司	8	8
沈阳东软系统集成工程有限公司	2	2
国瑞数码零点实验室	188	188
山东华鲁科技发展股份有限公司	47	47
远江盛邦（北京）网络安全科技股份有限公司	37	37

河南灵创电子科技有限公司	24	24
河南信安世纪科技有限公司	22	22
北京云科安信科技有限公司 (Seraph 安全实验室)	18	18
北京华云安信息技术有限公司	17	17
山东云天安全技术有限公司	15	15
内蒙古奥创科技有限公司	13	13
南京众智维信息科技有限公司	13	13
杭州海康威视数字技术股份有限公司	10	10
北京顶象技术有限公司	10	10
山东道普测评技术有限公司	9	9
吉林谛听信息技术有限公司	9	9
北京天地和兴科技有限公司	8	8
安徽长泰信息安全服务有限公司	8	8
杭州迪普科技股份有限公司	6	6
广西等保安全测评有限公司	6	6
平安银河实验室	4	4
上海纽盾科技股份有限公司	3	3
上海观安信息技术股份有限公司	2	2
上海犀点意象网络科技有限公司	1	1
中科华威 (北京) 信息技术研究院	1	1
北京长亭科技有限公司	1	1
京东云安全	1	1

浙江安腾信息技术有限公司	1	1
北京智游网安科技有限公司	1	1
北京惠而特科技有限公司	1	1
北京卓识网安技术股份有限公司	1	1
北京安华金和科技有限公司	1	1
CNCERT 宁夏分中心	9	9
CNCERT 上海分中心	5	5
CNCERT 西藏分中心	2	2
CNCERT 浙江分中心	1	1
CNCERT 四川分中心	1	1
CNCERT 吉林分中心	1	1
个人	414	414
报送总计	4050	3165

本周漏洞按类型和厂商统计

本周，CNVD 收录了 465 个漏洞。应用程序 274 个，WEB 应用 112 个，操作系统 38 个，网络设备（交换机、路由器等网络端设备）27 个，智能设备（物联网终端设备）漏洞 6 个，数据库 4 个，安全产品 4 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	274
WEB 应用	112
操作系统	38
网络设备（交换机、路由器等网络端设备）	27
智能设备（物联网终端设备）漏洞	6
数据库	4
安全产品	4

本周CNVD漏洞数量按影响类型分布

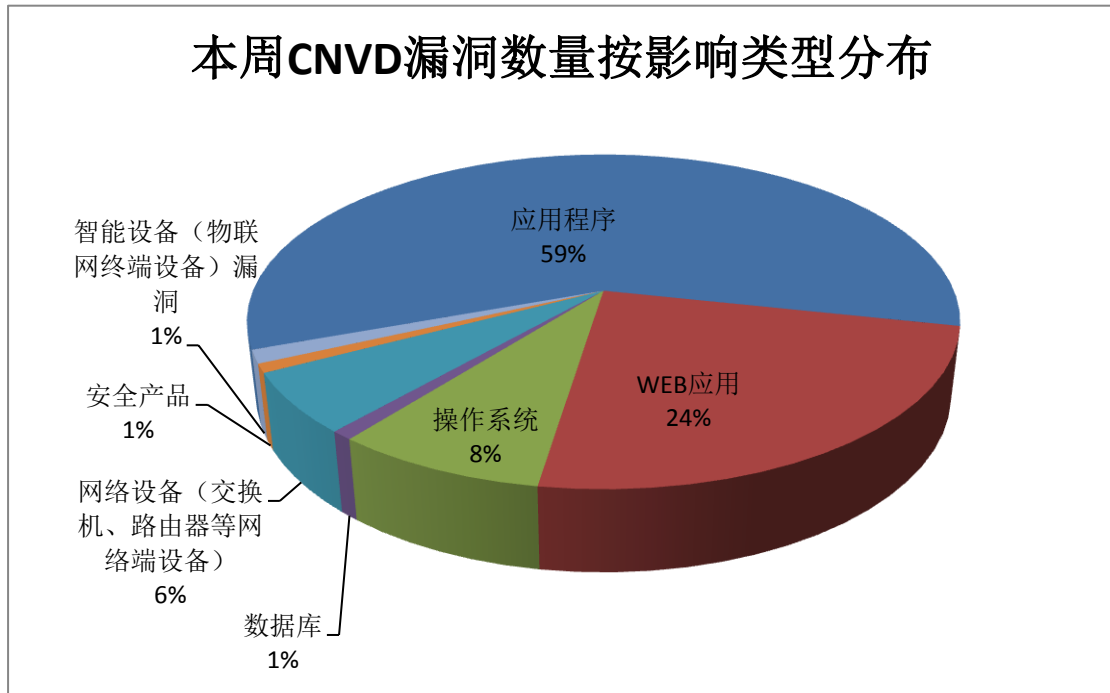


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Google、Microsoft 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	IBM	46	10%
2	Google	39	8%
3	Microsoft	26	6%
4	Cisco	12	3%
5	F5	12	3%
6	CloudBees	10	2%
7	WordPress	9	2%
8	JetBrains	8	2%
9	Atlassian	8	2%
10	其他	295	62%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，12 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“Cisco NX-OS 远程代码执行漏洞、Ubiquiti Networks EdgeSwitch 操作系统命令注入漏洞、Atlassian Confluence XSS 漏洞、Citrix Systems Xe

nMobile Server 访问控制错误漏洞”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/>

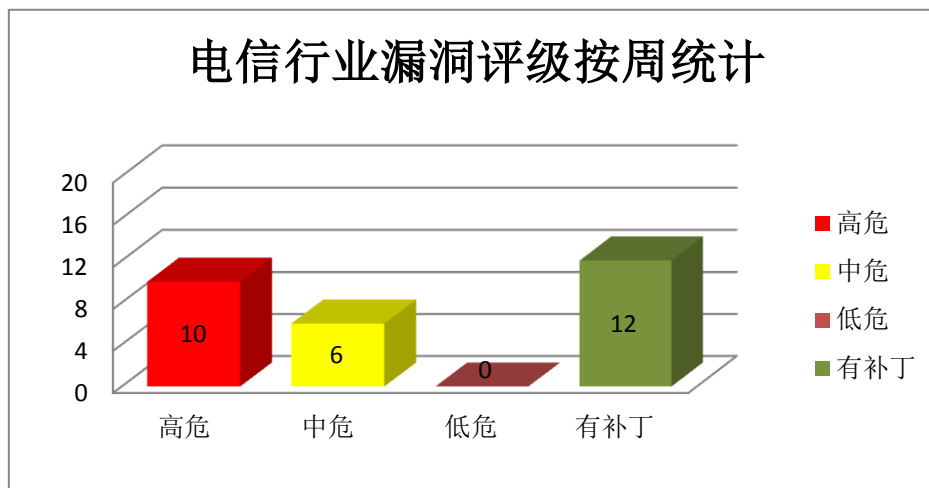


图 3 电信行业漏洞统计

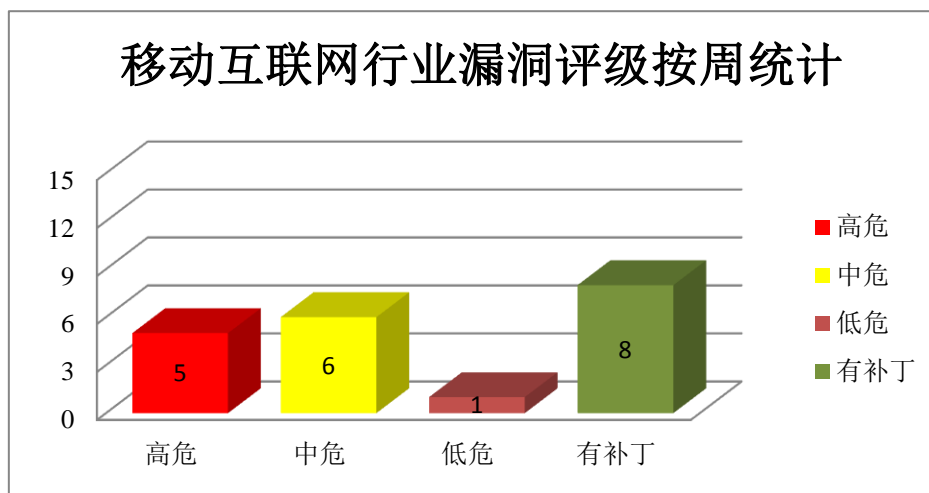


图 4 移动互联网行业漏洞统计

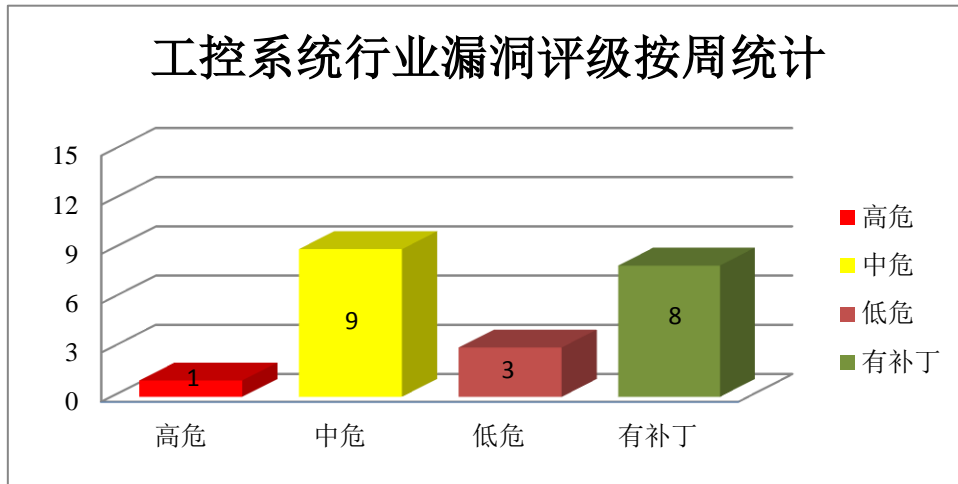


图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，上述产品被披露存在安全绕过漏洞，攻击者可利用漏洞绕过安全限制。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2020-49907、CNVD-2020-49909、CNVD-2020-49908、CNVD-2020-49912、CNVD-2020-49911、CNVD-2020-49910、CNVD-2020-49914、CNVD-2020-49913）。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-2020-49907>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49909>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49908>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49912>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49911>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49910>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49914>
<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49913>

2、Cisco 产品安全漏洞

Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网）解决方案的管理软件。Cisco Prime License Manager Software 是一套用于 Cisco 产品的许可证管理软件。Cisco IOS 和 Cisco IOS XR 都是为其网络设备开发的操作系统。Cisco NX-OS 是适用于 Cisco Nexus 系列以太网交换机和 MDS 系

列光纤通道存储区域网络交换机的网络操作系统。Cisco Connected Mobile Experiences (CMX)是一种智能 Wi-Fi 解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 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 SD-WAN vManage Software 输入验证错误漏洞、Cisco Prime License Manager Software 信任管理问题漏洞、Cisco IOS 和 Cisco IOS XR 资源管理错误漏洞、Cisco NX-OS 远程代码执行漏洞、Cisco NX-OS 拒绝服务漏洞（CNVD-2020-49933、CNVD-2020-50288）、Cisco NX-OS 命令注入漏洞（CNVD-2020-49932）、Cisco Connected Mobile Experiences 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-2020-49554>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49555>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49897>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49931>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49933>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49932>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-50153>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-50288>

3、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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 Excel 是一款 Office 套件中的电子表格处理软件。Microsoft Outlook 是一套电子邮件应用程序。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。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2020-49360、CNVD-2020-49359、CNVD-2020-49358）、Microsoft Windows 和 Microsoft Windows Server 远程代码执行漏洞（CNVD-2020-49363）、Microsoft Excel 内存破坏代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-50145、CNVD-2020-49506）、Microsoft Outlook 代码执行漏洞。其中，除“Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2020-49360、CNVD-2020-49359）”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-2020-49360>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49359>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49358>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49363>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49506>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-50118>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-50145>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-50158>

4、IBM 产品安全漏洞

IBM i2 Analysts Notebook 是美国 IBM 公司的一款数据可视化分析工具。IBM Sterling Connect: Direct 是一套基于文件的点对点文件传输解决方案。IBM Security Guardium Data Encryption (GDE)提供了一组模块化的加密解决方案，可帮助安全团队有效地实现整个组织的静态数据安全性。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，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：IBM i2 Analysts Notebook 缓冲区溢出漏洞（CNVD-2020-49391、CNVD-2020-49392、CNVD-2020-49393、CNVD-2020-49394、CNVD-2020-49395）、IBM Sterling Connect:Direct for UNIX 栈缓冲区溢出漏洞、IBM Security Guardium Data Encryption (GDE)硬编码凭据漏洞、IBM Security Guardium Data Encryption (GDE)任意命令执行漏洞。其中，“IBM Sterling Connect:Direct for UNIX 栈缓冲区溢出漏洞、IBM Security Guardium Data Encryption (GDE)硬编码凭据漏洞、IBM Security Guardium Data Encryption (GDE)任意命令执行漏洞”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-2020-49391>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49392>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49393>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49394>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49395>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49512>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49942>

<https://www.cnvd.org.cn/flaw/show/CNVD-2020-49945>

5、Red Hat oVirt 跨站脚本漏洞

Red Hat oVirt 是美国红帽（Red Hat）公司的一套开源的虚拟化管理平台，是 RHEV（企业虚拟化平台）的开源版本，由 ovirt-node 客户端和 ovirt-engine 管理端组成。本周，Red Hat oVirt 被披露存在跨站脚本漏洞。远程攻击者可利用该漏洞实施钓鱼攻击，窃取用户 cookie 或其他敏感信息，或冒充其他用户。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-2020-49701>

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-2020-49476	FasterXML jackson-databind 代码问题漏洞 (CNVD-2020-49476)	高	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/2462
CNVD-2020-49483	Apache SkyWalking SQL 注入漏洞 (CNVD-2020-49483)	高	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/r6f3a934ebc54585d8468151a494c1919dc1ee2cccaf237ec434dbbd6@%3Cdev.skywalking.apache.org%3E
CNVD-2020-49536	Contiki-NG 缓冲区溢出漏洞 (CNVD-2020-49536)	高	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/mjurczak/contiki-ng/tree/bugfix/snmp-engine
CNVD-2020-49571	Foxit Studio Photo PSD 越界写漏洞	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.foxitsoftware.com/support/security-bulletins.html
CNVD-2020-49574	Red Hat keycloak 资源管理错误漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://access.redhat.com/errata/RHSA-2020:3495
CNVD-2020-50256	Micro Focus Secure Messaging Gateway 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: https://support.microfocus.com/kb/doc.php?id=7024775
CNVD-2020-50286	F5 BIG-IP iControl REST 跨站请求伪造漏洞	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://support.f5.com/csp/article/K20606443
CNVD-2020-50496	Dell EMC Data Protection Advisor 操作系统命令注入漏洞	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.dell.com/support/security/zh-cn/details/542719/DSA-2020-081-Dell-EMC-Data-Protection-Advisor-OS-Command-Injection-Vulnerability
CNVD-2020-50498	McAfee Network Security Management 信息泄露漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接:

	(CNVD-2020-50498)		https://kc.mcafee.com/corporate/index?page=content&id=SB10322
CNVD-2020-50534	openSIS 远程代码执行漏洞 (CNVD-2020-50534)	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://opensis.com/

小结: 本周, Google 产品被披露存在多个漏洞, 攻击者可利用漏洞绕过安全限制。此外, Cisco、Microsoft、IBM 等多款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, 导致拒绝服务, 缓冲区溢出等。另外, Red Hat oVirt 被披露存在跨站脚本漏洞。远程攻击者可利用该漏洞实施钓鱼攻击, 窃取用户 cookie 或其他敏感信息, 或冒充其他用户。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 Vanguard 跨站脚本漏洞

验证描述

WordPress 是 WordPress 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。Vanguard 是使用在其中的一个自由职业网站主题插件。

WordPress Vanguard 2.1 版本中存在跨站脚本漏洞, 该漏洞源于 WEB 应用缺少对客户端数据的正确验证, 攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接: <https://packetstormsecurity.com/files/157099/Vanguard-2.1-Cross-Site-Scripting.html>

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2020-49523>

信息提供者

恒安嘉新(北京)科技股份公司

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. 美国国防部披露了严重漏洞

美国国防部 9 月 4 日, 披露了有关其基础架构上四个安全漏洞的详细信息。其中两

个具有高严重性等级，而其他两个则获得了严重评分。

参考链接：<https://www.bleepingcomputer.com/news/security/us-department-of-defense-discloses-critical-and-high-severity-bugs/>

2. Magento 的插件 Magmi 存在漏洞，容易劫持管理员会话

Magento 的 Magmi 插件中仍然存在跨站点请求伪造（CSRF）漏洞。黑客可以诱使经过身份验证的管理员点击恶意链接，从而利用该漏洞在运行 Magmi（Magento Mass Importer）的服务器上执行任意代码。

参考链接：<https://www.bleepingcomputer.com/news/security/magento-plugin-magmi-vulnerable-to-hijacking-admin-sessions/>

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