国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 09 月 30 日-2019 年 10 月 13 日 **2019 年第 40、41 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 488 个，其中高危漏洞 116 个、中危漏洞 322 个、低危漏洞 50 个。漏洞平均分值为 5.82。本周收录的漏洞中，涉及 0day 漏洞 157 个（占 32%），其中互联网上出现“Joomla! configuration.php 文件 RCE 漏洞、Zoho ManageEngine OpManager SQL 注入漏洞（CNVD-2019-34852）”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 4763 个，与上周（3148 个）环比增长 51%。

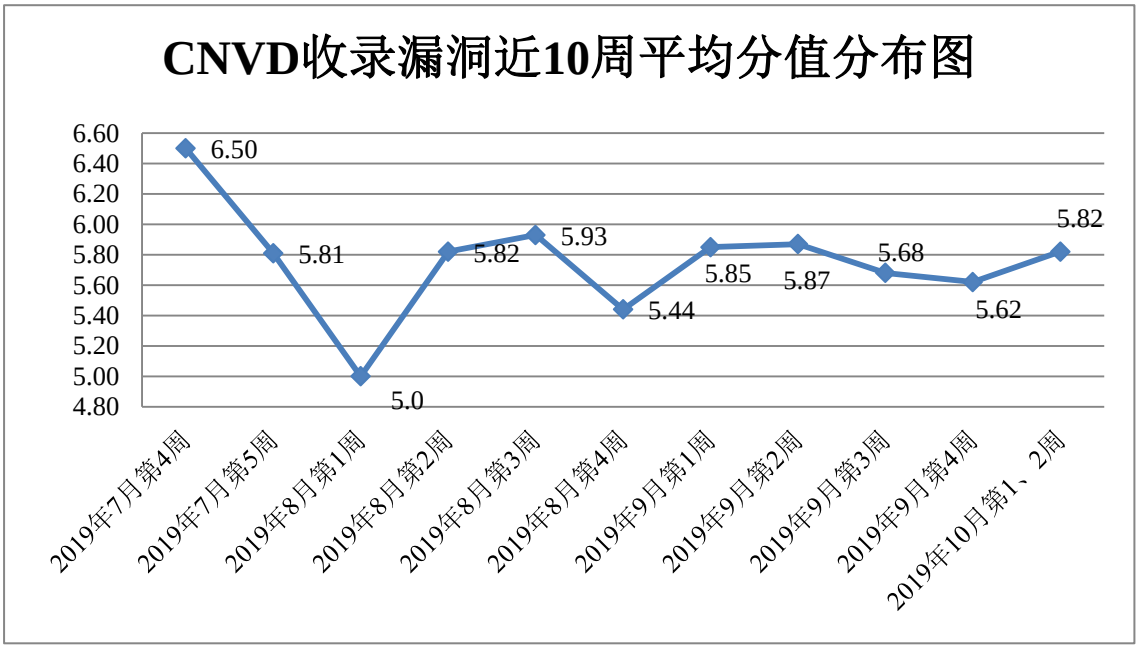

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 4 起，向银行、保险、能源等重要行业单位通报漏洞事件 13 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 429 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 110 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 25 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：

中国铁建重工集团股份有限公司、北京米尔伟业科技有限公司、淄博闪灵网络科技有限公司、国药控股陕西有限公司、青岛商至信网络科技有限公司、山东城通科技有限公司、北京正量网科技有限公司、广州恒企教育科技有限公司、北京泰克贝思科技股份有限公司、上海茸易科技有限公司、成都康菲顿特网络科技有限公司、北京世纪葵花数字传媒技术有限公司、北京昆仑通态自动化软件科技有限公司、深圳市永泰新欣科技有限公司、淮南市银泰软件科技有限公司、揭阳市集科计算机网络有限公司、成都火狐狸科技有限公司、南昌蓝智科技有限公司、丝路之约（北京）文化传媒有限公司、上海泛微网络科技股份有限公司、北京顺风益族科技有限公司、浙大正呈科技有限公司、国药控股北京康辰生物医药公司、郑州微口网络科技有限公司、惠州掌尚传橙新媒体有限公司、广州九尾信息科技有限公司 、中国中铁隧道集团第五建筑有限公司、上海甲鼎信息技术有限公司、自贡天启网络系统有限公司、成都用我在线科技发展有限公司、北京良精志诚科技有限责任公司、广州拓波软件科技有限公司、中国中铁电气化局集团公司、北京正影网络科技有限公司、中国化学工程第七建设有限公司、国药控股浙江有限公司、资海科技集团、国家农业信息化工程技术研究中心、中国银行间市场交易商协会、中国城乡统筹科学发展办公室、中国民主同盟、闻泰网络、为因软件、Adobe、Xnview、MayiCMS、YXcms、ZZCMS、YCCMS、ShuipFCMS、好 123、SeaCMS、MonkeyCode 和 XnView 公司。

本周，CNVD 发布了《关于 QEMU-KVM 虚拟机存在内核逃逸漏洞的安全公告》、《关于泛微 e-cology OA 系统存在 SQL 注入漏洞的安全公告》和《Microsoft 发布 2019 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/5233

https://www.cnvd.org.cn/webinfo/show/5235

https://www.cnvd.org.cn/webinfo/show/5237

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北北京天融信网络安全技术有限公司、华为技术有限公司、哈尔滨安天科技集团股份有限公司、四川无声信息技术有限公司、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。远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、山东云天安全技术有限公司、南京众智维信息科技有限公司、任子行网络技术股份有限公司、山石网科通信技术股份有限公司、北京君

信安科技有限公司、北京圣博润高新技术股份有限公司、北京智游网安科技有限公司、成都安美勤信息技术股份有限公司、河南信安世纪科技有限公司、上海端御信息科技有限公司、郑州赛欧思科技有限公司及其他个人白帽子向 CNVD 提交了 4763 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 3932 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）	1894	1894
斗象科技（漏洞盒子）	1403	1403
上海交大	635	635
北京天融信网络安全技术有限公司	385	14
华为技术有限公司	378	0
哈尔滨安天科技集团股份有限公司	241	0
四川无声信息技术有限公司	107	107
深信服科技股份有限公司	105	0
北京启明星辰信息安全技术有限公司	82	0
北京神州绿盟科技有限公司	64	9
新华三技术有限公司	56	0
中国电信集团系统集成有限责任公司	55	55
恒安嘉新(北京)科技股份公司	50	0
西安四叶草信息技术有限公司	26	26
北京数字观星科技有限公司	20	0
北京知道创宇信息技术股份有限公司	8	2
南京联成科技发展股份有限公司	5	5

厦门服云信息科技有限公司	1	1
中新网络信息安全股份有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	150	150
国瑞数码零点实验室	84	84
山东云天安全技术有限公司	57	57
南京众智维信息科技有限公司	54	54
任子行网络技术股份有限公司	20	20
山石网科通信技术股份有限公司	11	11
北京君信安科技有限公司	7	7
西门子（中国）有限公司	4	0
北京圣博润高新技术股份有限公司	4	4
北京智游网安科技有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
河南信安世纪科技有限公司	2	2
上海端御信息科技有限公司	2	2
郑州赛欧思科技有限公司	1	1
CNCERT 天津分中心	23	23
CNCERT 四川分中心	5	5
CNCERT 江西分中心	2	2
CNCERT 宁夏分中心	1	1
个人	184	184
报送总计	6131	4763

本周漏洞按类型和厂商统计

本周，CNVD 收录了 488 个漏洞。应用程序 305 个，WEB 应用 81 个，操作系统 40 个，智能设备（物联网终端设备）30 个，安全产品 13 个，网络设备（交换机、路由器等网络端设备）12 个，数据库 7 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	305
WEB 应用	81
操作系统	40
智能设备（物联网终端设备）	30
安全产品	13
网络设备（交换机、路由器等网络端设备）	12
数据库	7

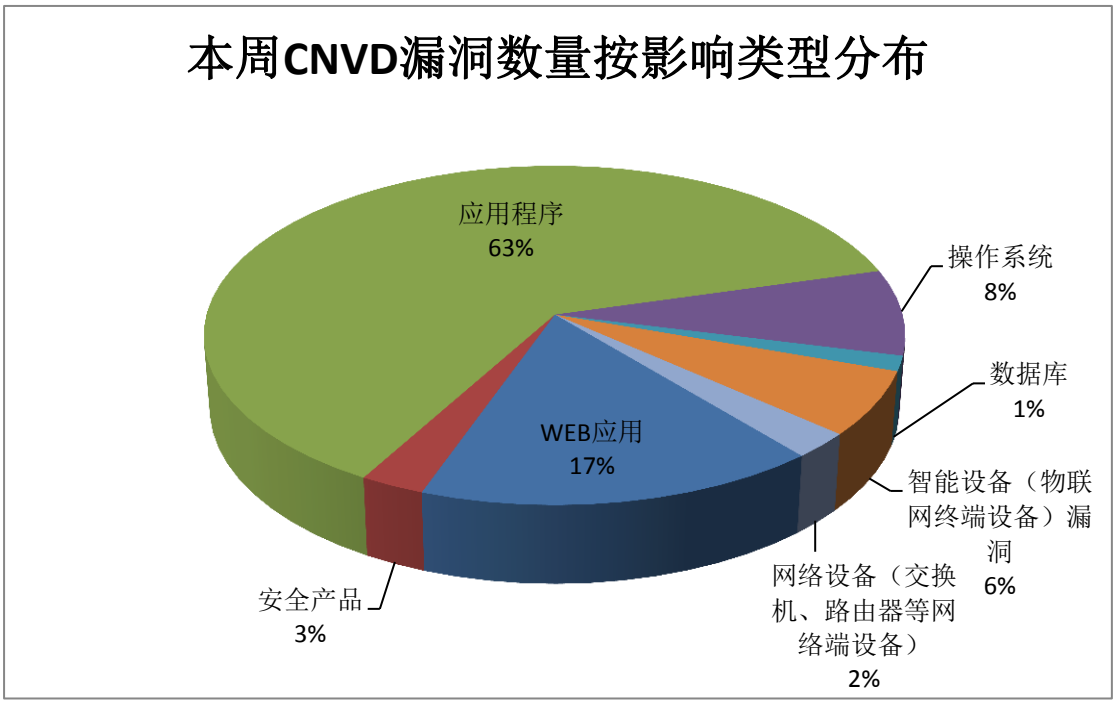

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Sugarcrm、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	WordPress	31	6%
2	Sugarcrm	30	6%
3	Microsoft	26	5%

4	Oracle	24	5%
5	Google	23	5%
6	Cisco	22	5%
7	cPanel	22	5%
8	IBM	19	4%
9	CloudBees	16	3%
10	其他	275	56%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，28 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Cisco ASR 900 Cisco IOS XE 输入验证错误漏洞、Microsoft Windows 和 Windows Server 远程执行代码漏洞、Siemens SIMATIC WinAC RTX (F) 2010 拒绝服务漏洞、Google Android VPN 信息泄露漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，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/

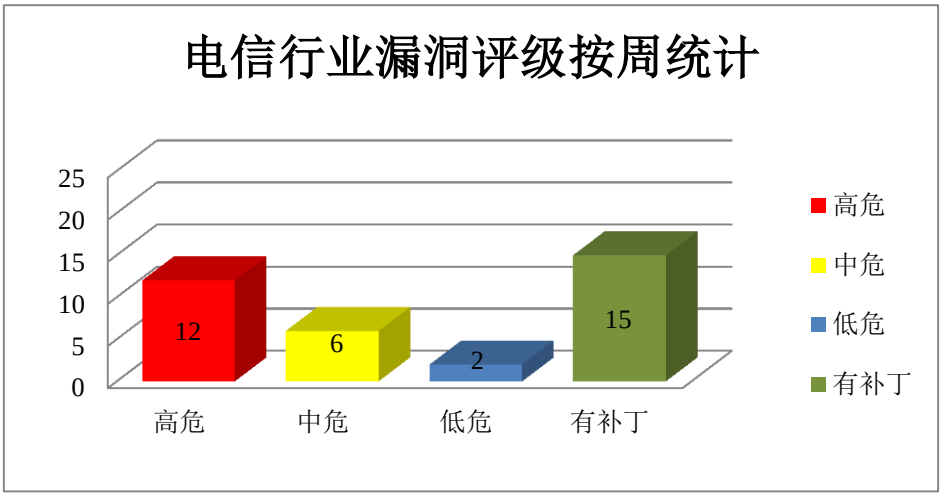

图 3 电信行业漏洞统计

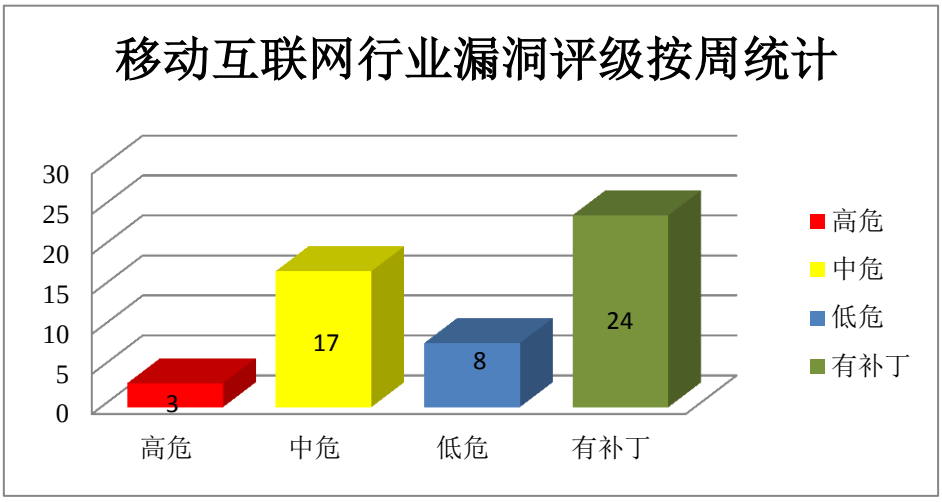

图 4 移动互联网行业漏洞统计

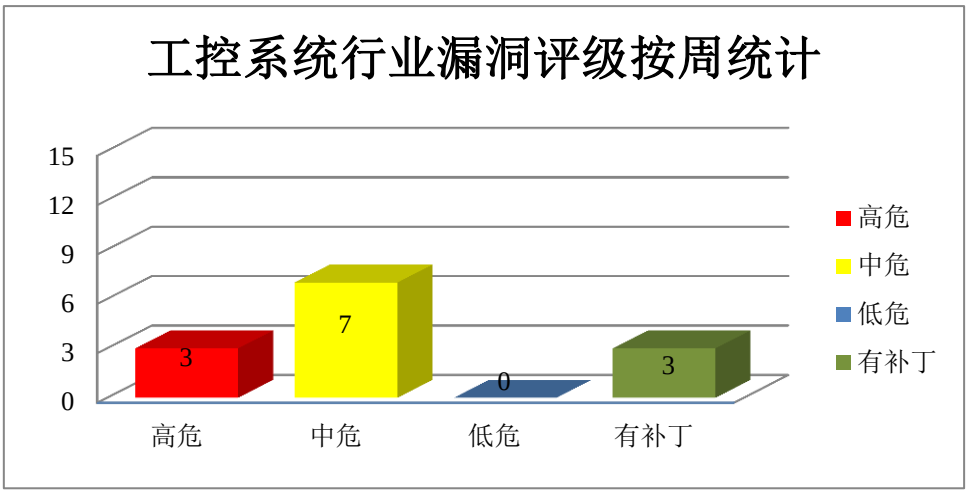

图 5 工控系统行业漏洞统计

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、泛微 e-cology OA 系统 Wo***接口存在 SQL 注入漏洞

泛微协同管理应用平台（e-cology）是一套兼具企业信息门户、知识管理、数据中心、工作流管理、人力资源管理、客户与合作伙伴管理、项目管理、财务管理、资产管理功能的协同商务平台。本周，该产品被披露存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

CNVD 收录的相关漏洞包括：泛微 e-cology OA 系统 Wo***接口存在 SQL 注入漏洞。上述漏洞的综合评级为“高危”。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34241

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。ChakraCore 是使用在 Edge 浏览器中的一个开源的 ChakraJava Script 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft SharePoint 是一套企业业务协作平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 输入验证错误漏洞、Microsoft Windows 和 Windows Server Jet Database Engine 远程代码执行漏洞、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2019-34581）、Microsoft Windows 和 Windows Server 远程执行代码漏洞、Microsoft Windows Hyper-V 远程执行代码漏洞（CNVD-2019-34587）、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2019-34741）、Microsoft Edge 和 ChakraCore 内存破坏漏洞（CNVD-2019-34742）、Microsoft SharePoint 权限提升漏洞（CNVD-2019-34774）。其中，除“Microsoft SharePoint 权限提升漏洞（CNVD-2019-34774）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34577
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34578
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34581
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34585
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34587
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34741
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34742
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34774

3、Cisco 产品安全漏洞

Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。本周，上述产品被披露存在 SQL 注入漏洞，攻击者可通过发送特制的 SQL 查询利用该漏洞查看信息并在底层操作系统中执行命令。

CNVD 收录的相关漏洞包括：Cisco Firepower Management Center SQL 注入漏洞（CNVD-2019-34714、CNVD-2019-34719、CNVD-2019-34731、CNVD-2019-34732、CNVD-2019-34736、CNVD-2019-34733、CNVD-2019-34737、CNVD-2019-34738）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34714
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34719

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34731

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34732

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34736

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34733

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34737

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34738

4、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在信息泄露和拒绝服务漏洞，攻击者可利用漏洞获取受影响组件敏感信息，导致拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 拒绝服务漏洞（CNVD-2019-34131、CNVD-2019-34133）、Google Android 信息泄露漏洞（CNVD-2019-34132、CNVD-2019-34134、CNVD-2019-34398、CNVD-2019-34399、CNVD-2019-34400）、Google Android VPN 信息泄露漏洞。其中，“Google Android 拒绝服务漏洞（CNVD-2019-34131）、Google Android VPN 信息泄露漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34131

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34132

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34133

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34134

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34398

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34399

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34400

http://www.cnvd.org.cn/flaw/show/CNVD-2019-34469

5、Oracle 产品安全漏洞

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。Oracle GraalVM 是一套使用 Java 语言编写的即时编译器。Oracle Hospitality Applications 是一套用于酒店管理的业务应用程序、服务器和存储解决方案。Oracle Hyperion 是一套财务建模应用软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle Fusion Middleware BI Publisher 组件信息泄露漏洞、Oracle Fusion Middleware HTTP Server 组件访问控制错误漏洞、Oracle Fusion Middleware Identity Manager 组件访问控制错误漏洞、Oracle GraalVM 访问控制错误漏洞、Oracle Hospitality Applications Hospitality Suite8 组件信息泄露漏洞、Oracle

Hyperion Hyperion Planning 组件访问控制错误漏洞、Oracle Fusion Middleware BI Publisher 信息泄露漏洞、Oracle Fusion Middleware SOA Suite 访问控制错误漏洞。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34695
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34696
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34697
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34694
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34698
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34699
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34708
http://www.cnvd.org.cn/flaw/show/CNVD-2019-34706

5、Linear eMerge 50P/5000P 文件上传漏洞

Linear eMerge 50P/5000P 是 Nortek Security＆Control 推出的通过浏览器管理的门禁安全系统。本周，Linear eMerge 50P/5000P 被披露存在文件上传漏洞。攻击者可利用该漏洞将具有任意扩展名的文件上传到应用程序的 Web 根目录中的目录，并以 Web 服务器的权限执行上传的文件。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34615

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-2019-33857	Red Lion Controls Crimson 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.redlion.net
CNVD-2019-34126	Couchbase Server 代码注入漏洞	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.couchbase.com/resources/security#SecurityAlerts
CNVD-2019-34371	Apple Xcode ld64 组件任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT210609
CNVD-2019-34384	Suricata 缓冲区溢出漏洞（CNVD-2019-34384）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://suricata-ids.org/2019/09/24/suricata-4-1-5-released/

CNVD-2019-34386	ZTE ZXV10 B860A 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011263
CNVD-2019-34595	Siemens SIMATIC WinAC RTX (F) 2010 拒绝服务漏洞	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-878278.pdf
CNVD-2019-34681	GPAC MP4Box 堆溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/gpac/gpac/commit/bceb03fd2be95097a7b409ea59914f332fb6bc86
CNVD-2019-34755	Suricata 越界读取漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://suricata-ids.org/2018/07/18/suricata-4-0-5-available/
CNVD-2019-34769	Xen 拒绝服务漏洞（CNVD-2019-34769）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://xenbits.xen.org/xsa/advisory-292.html
CNVD-2019-35033	Pengutronix Barebox 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.pengutronix.de/cgit/barebox/commit/fs/nfs.c?h=next&id=574ce994016107ad8ab0f845a785f28d7eaa5208

小结：本周，泛微 e-cology OA 系统 Wo***接口被披露存在 SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感信息。此外，Microsoft、Cisco、Google、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，提升权限，执行任意代码，导致拒绝服务等。另外，Linear eMerge 50P/5000P 被披露存在文件上传漏洞。攻击者可利用该漏洞将具有任意扩展名的文件上传到应用程序的 Web 根目录中的目录，并以 Web 服务器的权限执行上传的文件。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、Joomla! configuration.php 文件 RCE 漏洞

验证描述

Joomla!是一套使用 PHP 和 MySQL 开发的开源、跨平台的内容管理系统(CMS)。

Joomla! configuration.php 文件存在 RCE 漏洞。攻击者可利用漏洞写入一句话木马，获得服务器权限。

验证信息

POC 链接：https://github.com/momika233/Joomla-3.4.6-RCE/blob/master/Joomla-3.4.6-RCE.py

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-34135

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. 苹果 macOS 终端工具 iTerm2 被发现一个存在 7 年的重大漏洞

iTerm2 是终端模拟器，被许多开发者与系统管理员广泛使用，不少人甚至会用它来处理一些不受信任的数据，据了解，这个漏洞在 iTerm2 中已存在长达 7 年，目前分配到的编号为 CVE-2019-9535。这个漏洞可以让攻击者在使用者电脑上执行命令。

参考链接：https://www.ithome.com/0/449/968.htm

2. NSA 的逆向工程框架 Ghidra 中曝出代码执行漏洞

安全研究人员发现了一个代码执行漏洞，该漏洞会通过 9.0.4 版本的 Ghidra 运行，被命名为 CVE-2019-16941，攻击者可以利用该漏洞在受影响的应用程序上下文中执行任意代码。研究人员发现，只有在启用实验模式后才能利用此漏洞。

参考链接：https://securityaffairs.co/wordpress/92280/hacking/ghidra-code-execution-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