国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 05 月 13 日-2019 年 05 月 19 日 **2019 年第 20 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 363 个，其中高危漏洞 111 个、中危漏洞 203 个、低危漏洞 49 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 141 个（占 39%），其中互联网上出现“WordPress 插件 Form Maker SQL 注入漏洞、PHP-Fusion 'Edit Profile'远程代码执行漏洞”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 1672 与上周（3387 个）环比下降 51%。

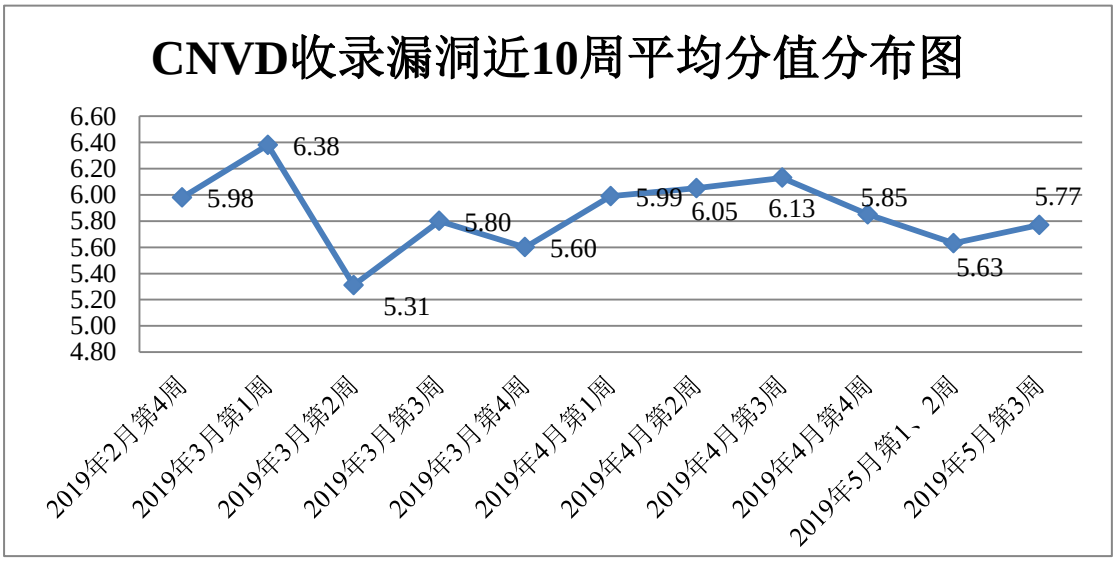

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 起，向银行、保险、能源等重要行业单位通报漏洞事件 14 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 344 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 12 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：

北京火绒网络科技有限公司、苏州聚尚网络科技有限公司、郑州路之易科技有限公司、厦门建发房地产集团有限公司、深圳市锟铻科技有限公司、上海茸易科技有限公司、深圳市物联锁科技有限公司、泰州智搜网络科技有限公司、南京尚网网络科技有限公司、四川蜀品天下信息技术有限公司、迈普通信技术股份有限公司、福州凌夕网络科技有限公司、深圳搜豹网络有限公司、南昌百恒信息技术有限公司、开开物联（北京）信息技术有限公司、邳州天目网络科技有限公司、厦门易尔通网络科技有限公司、浪潮集团有限公司、中国中铁隧道股份有限公司、湖南心艾网络科技有限公司、成都动力无限科技有限公司、浙江逆天网络科技有限责任公司　北京市建设工程发包承包交易中心、中国科技金融促进会、北京中交诚通工程技术研究院、帝国软件、微派科技、鲶鱼 CMS、易优 CMS、爱客 CMS、EarCMS、JeeWeb 、Joomla、Nsasoft US、WellCMS、Socusoft。

本周，CNVD 发布了《Microsoft 发布 2019 年 5 月安全更新》、《关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/5019

http://www.cnvd.org.cn/webinfo/show/5021

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、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、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。任子行网络技术股份有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、中新网络信息安全股份有限公司、泰山信息科技有限公司、南京联成科技发展股份有限公司、上海并擎软件科技有限公司、北京圣博润高新技术股份有限公司、河南信安世纪科技有限公司、广州市眯眼猫信息科技有限公司、山东华鲁科技发展股份有限公司、新疆海狼科技有限公司、山石网科通信技术有限公司、长春嘉诚信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 1672 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1116 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）	737	737
奇安信网神（补天平台）	379	379

哈尔滨安天科技集团股份有限公司	232	0
华为技术有限公司	192	0
北京天融信网络安全技术有限公司	111	12
新华三技术有限公司	100	0
恒安嘉新(北京)科技股份公司	86	0
深信服科技股份有限公司	81	0
北京启明星辰信息安全技术有限公司	42	0
北京神州绿盟科技有限公司	21	0
中国电信集团系统集成有限责任公司	21	0
北京知道创宇信息技术股份有限公司	13	12
百度安全响应中心（BSRC）	1	1
沈阳东软系统集成工程有限公司	1	1
任子行网络技术股份有限公司	143	143
国瑞数码零点实验室	89	89
内蒙古奥创科技有限公司	44	44
中新网络信息安全股份有限公司	30	30
泰山信息科技有限公司	27	27
南京联成科技发展股份有限公司	18	18
上海并擎软件科技有限公司	5	5
北京圣博润高新技术股份有限公司	3	3
河南信安世纪科技有限公司	2	2
广州市眯眼猫信息科技有限公司	2	2

山东华鲁科技发展股份有限公司	2	2
新疆海狼科技有限公司	2	2
山石网科通信技术有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
CNCERT 天津分中心	7	7
CNCERT 海南分中心	3	3
CNCERT 吉林分中心	3	3
CNCERT 广西分中心	1	1
CNCERT 贵州分中心	1	1
个人	146	146
报送总计	2547	1672

本周漏洞按类型和厂商统计

本周，CNVD 收录了 363 个漏洞。应用程序 171 个，WEB 应用 94 个，操作系统 49 个，网络设备（交换机、路由器等网络端设备）25 个，安全产品 12 个，数据库 5 个，智能设备（物联网终端设备）漏洞 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	171
WEB 应用	94
操作系统	49
网络设备（交换机、路由器等网络端设备	25
安全产品	12
数据库	5
智能设备（物联网终端设备）漏洞	7

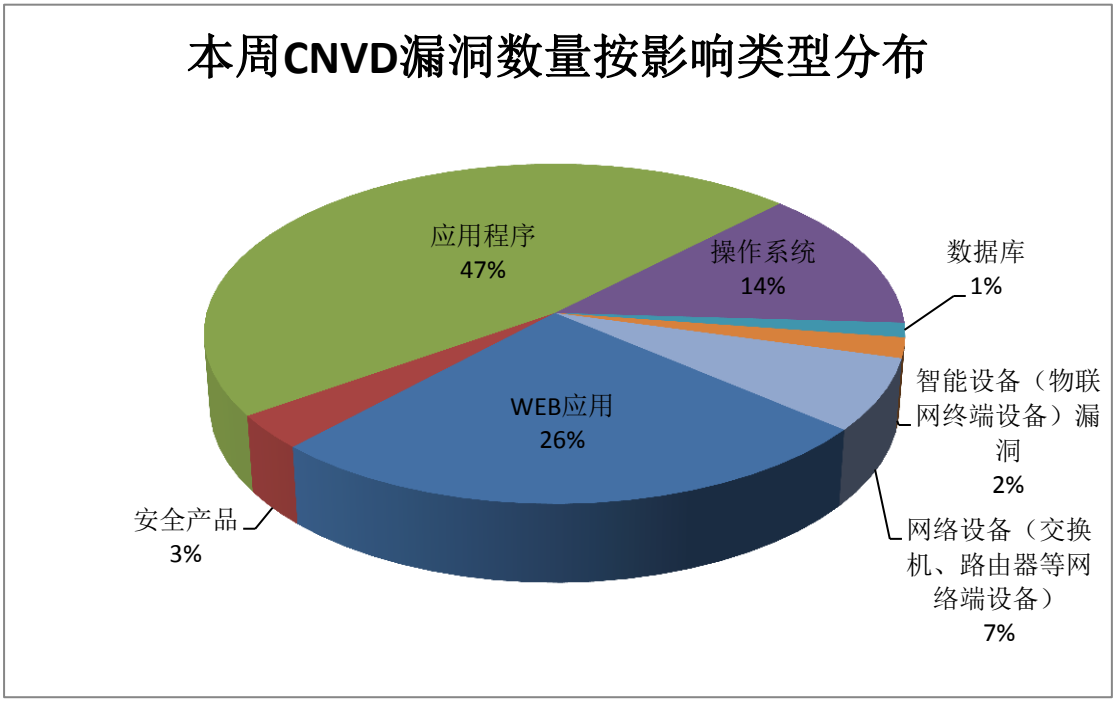

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Cisco、Foxit 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	Microsoft	42	12%
2	Cisco	33	9%
3	Foxit	22	6%
4	doorGets	17	5%
5	IBM	12	3%
6	ZyXEL	10	3%
7	Joomla!	9	2%
8	Orpak	6	2%
9	Cacti	5	1%
10	其他	207	57%

本周行业漏洞收录情况

本周，CNVD 收录了 40 个电信行业漏洞，6 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 NX-OS Software 和 Cisco FXOS Software 拒绝服务漏洞、多款 Cisco 产品输入验证错误漏洞、Cisco IOS 和 IOS XE ISDN 接口拒绝服务

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/

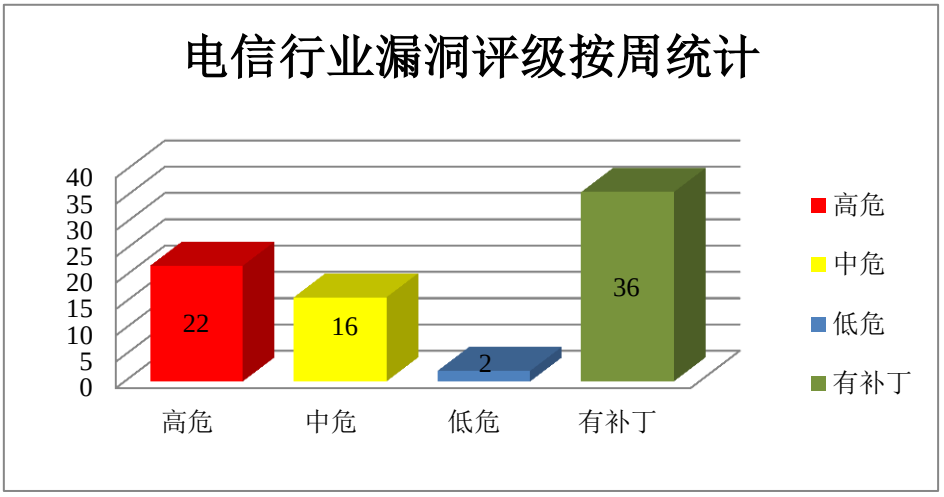

图 3 电信行业漏洞统计

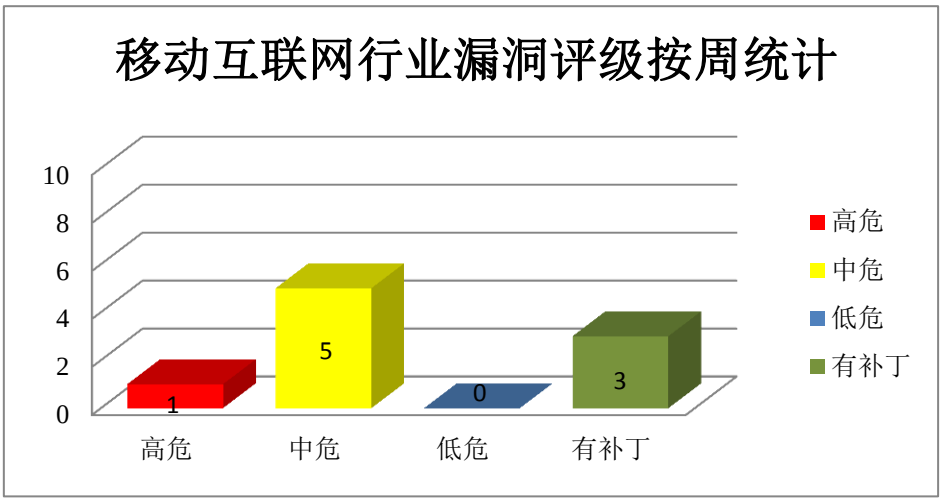

图 4 移动互联网行业漏洞统计

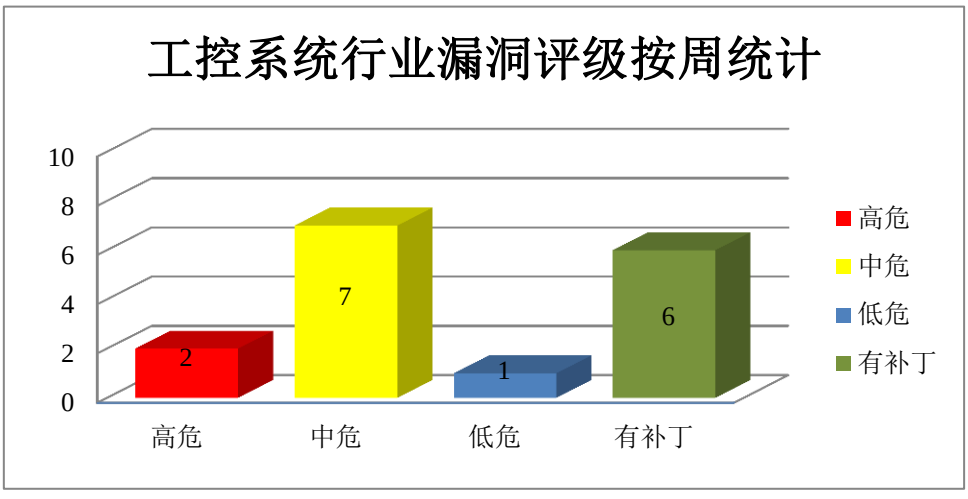

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Jet Database Engine 是一个底层数据库引擎。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Jet Database Engine 远程代码执行漏洞（CNVD-2019-14454、CNVD-2019-14455、CNVD-2019-14457、CNVD-2019-14456、CNVD-2019-14459、CNVD-2019-14458、CNVD-2019-14460、CNVD-2019-14462）。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-2019-14454
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14455
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14457
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14456
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14459
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14458
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14460
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14462

2、Cisco 产品安全漏洞

Cisco IOS 是一套为其网络设备开发的操作系统。Cisco NX-OS 是适用于思科 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。本周，上述产品被披露存在拒绝服务和命令注入漏洞，攻击者可利用漏洞执行任意命令，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS NAT64 拒绝服务漏洞、Cisco NX-OS 命令注入漏洞（CNVD-2019-14614、CNVD-2019-14613、CNVD-2019-14615、CNVD-2019-14619、CNVD-2019-14620、CNVD-2019-14621、CNVD-2019-14623）。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-2019-14103
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14614
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14613
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14615
http://www.cnvd.org.cn/flaw/show/CNVD-2019-14619

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14620

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14621

http://www.cnvd.org.cn/flaw/show/CNVD-2019-14623

3、Foxit 产品安全漏洞

Foxit Reader 和 Foxit PhantomPDF 都是一款 PDF 文档阅读器。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，执行任意命令等。

CNVD 收录的相关漏洞包括：Foxit Reader 和 Foxit PhantomPDF for Windows 缓冲区溢出漏洞（CNVD-2019-13808）、Foxit Reade 和 Foxit PhantomPDF for Windows 路径遍历漏洞、Foxit Reader 和 Foxit PhantomPDF for Windows 资源管理错误漏洞（CNVD-2019-13810）、Foxit Reader 和 Foxit PhantomPDF for Windows 越界写入漏洞（CNVD-2019-13812、CNVD-2019-13813、CNVD-2019-13817）、Foxit Reader 和 Foxit PhantomPDF for Windows 信息泄露漏洞（CNVD-2019-13811）、Foxit Reader 和 Foxit PhantomPDF for Windows 越界读取漏洞（CNVD-2019-13818）。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-2019-13808

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13807

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13810

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13812

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13811

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13813

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13817

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13818

4、doorGets 产品安全漏洞

doorGets 是一款免费开源内容管理系统。本周，该产品被披露存在 SQL 注入和敏感信息泄露漏洞，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：doorGets 敏感信息泄露漏洞（CNVD-2019-13789、CNVD-2019-13788、CNVD-2019-13791、CNVD-2019-13790、CNVD-2019-13793、CNVD-2019-13792）、doorGets SQL 注入漏洞（CNVD-2019-13795、CNVD-2019-13796）。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-2019-13789

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13788

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13791

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13790

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13793

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13792

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13795

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13796

5、ZyXEL NSA325 V2 跨站请求伪造漏洞

ZyXEL NSA325 V2 是一款网络存储设备。ZyXEL NSA325 V2 被披露存在跨站请求伪造漏洞。攻击者可借助特制的 HTTP 表单利用该漏洞执行状态更改操作。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-2019-13784

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-2019-13849	Magento 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://magento.com/
CNVD-2019-13852	lighttpd 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：https://redmine.lighttpd.net/issues/2945
CNVD-2019-13856	MikroTik RouterOS 目录遍历漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://mikrotik.com/download
CNVD-2019-14071	TYPO3 PharStreamWrapper 远程代码执行的漏洞	高	用户可联系供应商获得补丁信息：https://www.drupal.org/sa-core-2019-007
CNVD-2019-14074	IBM DB2 栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10741481
CNVD-2019-14086	Orpak SitOmat 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https：//support.zoho.com/portal/orpak
CNVD-2019-14241	Linux Kernel rds_tcp_kill_sock 竞争条件漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.0.8
CNVD-2019-14254	Domoticz SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/domoticz/domoticz/commit/ee70db46f81afa582c96b887b73

			bcd2a86feda00
CNVD-2019-14428	Bash 输入验证错误漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://git.savannah.gnu.org/cgit/bash.git/tree/CHANGES?h=bash-4.4-testing#n65
CNVD-2019-14430	Vdsm 任意命令执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://gerrit.ovirt.org/#/c/97659/

小结：本周，Microsoft 被披露存在堆溢出和越界读取漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、Foxit、doorGets 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，执行任意命令，发起拒绝服务攻击等。ZyXEL NSA325 V2 被披露存在跨站请求伪造漏洞。攻击者可借助特制的 HTTP 表单利用该漏洞执行状态更改操作。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、PHP-Fusion 'Edit Profile'远程代码执行漏洞

验证描述

PHP-Fusion 是一套基于 MySql 和 PHP 的开源轻量级内容管理系统。

PHP-Fusion 'Edit Profile'存在远程代码执行漏洞。攻击者可利用漏洞使用普通用户权限在系统中执行命令。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=33106

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-14278

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. 俄罗斯政府网站泄露 225 万用户护照和个人信息

多个俄罗斯政府网站泄露了超过 225 万公民、府雇员和政治家的个人和护照信息，任何人都可以下载。俄罗斯非政府组织 Informational Culture 的联合创始人 Ivan Begtin

发现并记录了泄漏事件。他调查了政府在线认证中心\50 个政府门户网站以及政府机构使用的电子投标平台。其中有 23 个网站泄露个人保险账号（SNILS：俄罗斯相当于社会安全号码）和 14 个泄露护照信息的网站。

Begtin 表示通过这些网站可以在线获得超过 225 万俄罗斯公民的数据，包括全名、职称和工作地点、电子邮件、税号、护照号等信息。虽然一部分泄漏数据难以识别并且需要从数字签名文件中提取元数据，但可以通过谷歌搜索政府网站上的开放网络目录找到一些数据。

参考链接：https://www.zdnet.com/article/russian-government-sites-leak-passport-and-personal-data-for-2-25-million-users/

2. 英特尔处理器新漏洞 ZombieLoad

在 Meltdown、Spectre 和 Foreshadow 之后，计算机科学家公开了英特尔处理器的新边信道攻击 ZombieLoad，攻击影响 2011 年之后发布的几乎所有英特尔处理器（包括 Core 和 Xeon），AMD 不受影响。这是一个硬件问题，因此漏洞利用代码可以工作在 Windows 和 Linux 等不同操作系统上。ZombieLoad 的漏洞利用同样是基于预测执行过程，通过利用 CPU 负荷返回值的旁路逻辑，去实现跨线程、权限边界和超线程的数据泄露。英特尔据报道曾试图推迟漏洞披露。

参考链接：https://www.solidot.org/story?sid=60611

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