国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 07 月 29 日-2019 年 08 月 04 日　　2019 年第 31 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 308 个，其中高危漏洞 82 个、中危漏洞 200 个、低危漏洞 26 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 41 个（占 13%），其中互联网上出现“Veeam ONE Reporter 跨站脚本漏洞、GetSimple CMS 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 2687 个，与上周（2259 个）环比增长 19%。

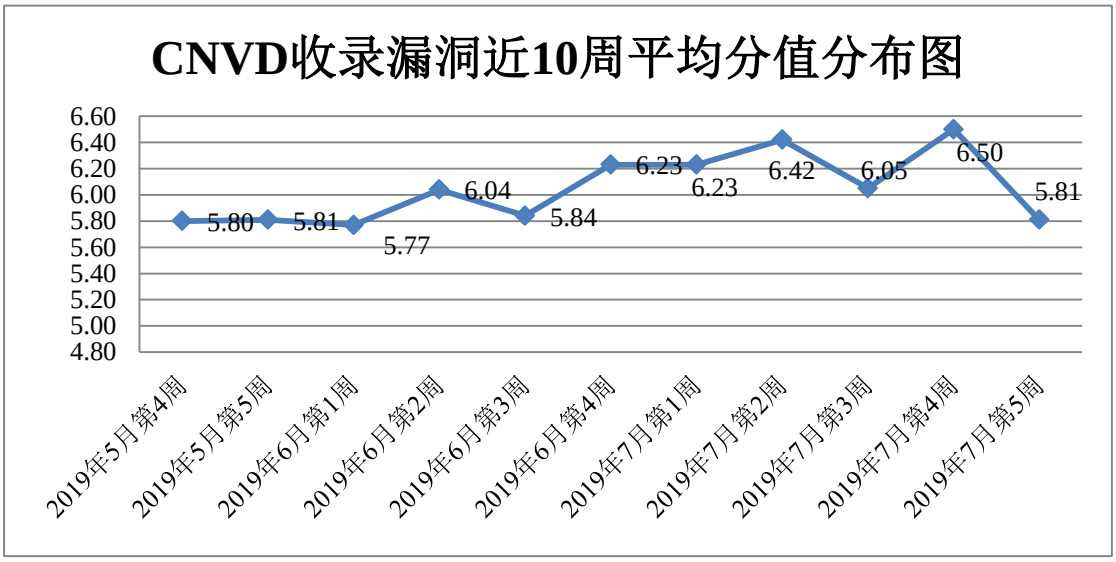

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向银行、保险、能源等重要行业单位通报漏洞事件 23 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 356 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 104 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 30 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：

深圳好生意网络工作室、嘉兴想天信息科技有限公司、浙江齐治科技股份有限公司、中冶智城（武汉）信息技术有限公司、苏州托普斯网络科技有限公司、中铁二局集团有限公司、中央储备粮青岛直属库有限公司、中国化学工程第九建设公司江苏分公司、桂林崇胜网络科技有限公司、北京爱奇艺新媒体科技有限公司、北京智量科技有限公司、北京火绒网络科技有限公司、湖南翱云网络科技有限公司、中船财务有限公司、国药控股云南有限公司、企炬-北京网站建设公司、上海同磊土木工程技术有限公司、西安三才科技实业有限公司、国药控股黄石有限公司、深圳市咨微信息科技有限公司、合肥梦扬科技有限公司、上海梦之路数字科技有限公司、陕西云企网络科技有限公司、陕西长银消费金融有限公司、内蒙古浩海商贸有限公司、上海茸易科技有限公司、中铁八局集团电务工程有限公司、西安华尚软件科技有限公司、太原迅易科技有限公司、大唐电信科技股份有限公司、北京春笛网络信息技术服务有限公司、航天数联信息技术（深圳）有限公司、南京苏迪科技有限公司、深圳市硕赢互动信息技术有限公司、海南赞赞网络科技有限公司、南京深图计算机技术有限公司、国药控股江西有限公司、四三九九网络股份有限公司、中国建筑一局（集团）有限公司、施耐德（Schneider Electric）、御宅男工作室、深圳市大数据资源管理中心、中国法院网、中国医药文化网、中国中医科学院、中国信息通信研究院、中国地震学会、中国交通运输协会、中国物资再生协会再制造分会、中国教育发展基金会、中国橡胶工业协会乳胶分会、中国残疾人联合会、中国儿童少年基金会中国外汇管理杂志社、ZZCMS、Zzzcms、iCMS、Notepad++和 Pluck CMS。

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、京天融信网络安全技术有限公司、为技术有限公司、川无声信息技术有限公司、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。国网思极检测技术（北京）有限公司、山信息科技有限公司、东云天安全技术有限公司、春嘉诚信息技术股份有限公司、瑞数码零点实验室、京众智维信息科技有限公司、东新潮信息技术有限公司、子行网络技术股份有限公司、京圣博润高新技术股份有限公司、海并擎软件科技有限公司、州锦行网络科技有限公司、南信安世纪科技有限公司、东华鲁科技发展股份有限公司、蒙古奥创科技有限公司、江盛邦（北京）网络安全科技股份有限公司、京智游网安科技有限公司、石网科通信技术有限公司、海银基信息安全技术股份有限公司、疆海狼科技有限公司及其他个人白帽子向 CNVD 提交了 2687 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 1726 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
奇安信网神（补天平台）	516	516
哈尔滨安天科技集团股份有限公司	274	0
北京天融信网络安全技术有限公司	265	12
华为技术有限公司	138	0
四川无声信息技术有限公司	101	101
深信服科技股份有限公司	88	0
恒安嘉新(北京)科技股份公司	55	2
新华三技术有限公司	54	0
西安四叶草信息技术有限公司	42	42
北京神州绿盟科技有限公司	38	3
中新网络信息安全股份有限公司	33	33
北京数字观星科技有限公司	21	0
厦门服云信息科技有限公司	17	0
杭州安恒信息技术股份有限公司	4	4
北京知道创宇信息技术股份有限公司	2	1
沈阳东软系统集成工程有限公司	2	2
百度安全响应中心（BSRC）	1	1
国网思极检测技术（北京）有限公司	110	110
泰山信息科技有限公司	88	88

山东云天安全技术有限公司	82	82
长春嘉诚信息技术股份有限公司	65	65
国瑞数码零点实验室	58	58
南京众智维信息科技有限公司	53	53
山东新潮信息技术有限公司	46	46
任子行网络技术股份有限公司	25	25
北京圣博润高新技术股份有限公司	15	15
上海并擎软件科技有限公司	12	12
广州锦行网络科技有限公司	11	11
河南信安世纪科技有限公司	9	9
山东华鲁科技发展股份有限公司	8	8
内蒙古奥创科技有限公司	6	6
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京智游网安科技有限公司	2	2
山石网科通信技术有限公司	2	2
上海银基信息安全技术股份有限公司	1	1
新疆海狼科技有限公司	1	1
CNCERT 山西分中心	5	5
CNCERT 西藏分中心	2	2
CNCERT 广西分中心	1	1
CNCERT 上海分中心	1	1
CNCERT 云南分中心	1	1

个人	153	153
报送总计	3621	2687

本周漏洞按类型和厂商统计

本周，CNVD 收录了 308 个漏洞。应用程序 173 个，操作系统 53 个，WEB 应用 51 个，网络设备（交换机、路由器等网络端设备）29 个，安全产品 1 个，智能设备（物联网终端设备）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	173
操作系统	53
WEB 应用	51
网络设备（交换机、路由器等网络端设备）	29
安全产品	1
智能设备（物联网终端设备）	1

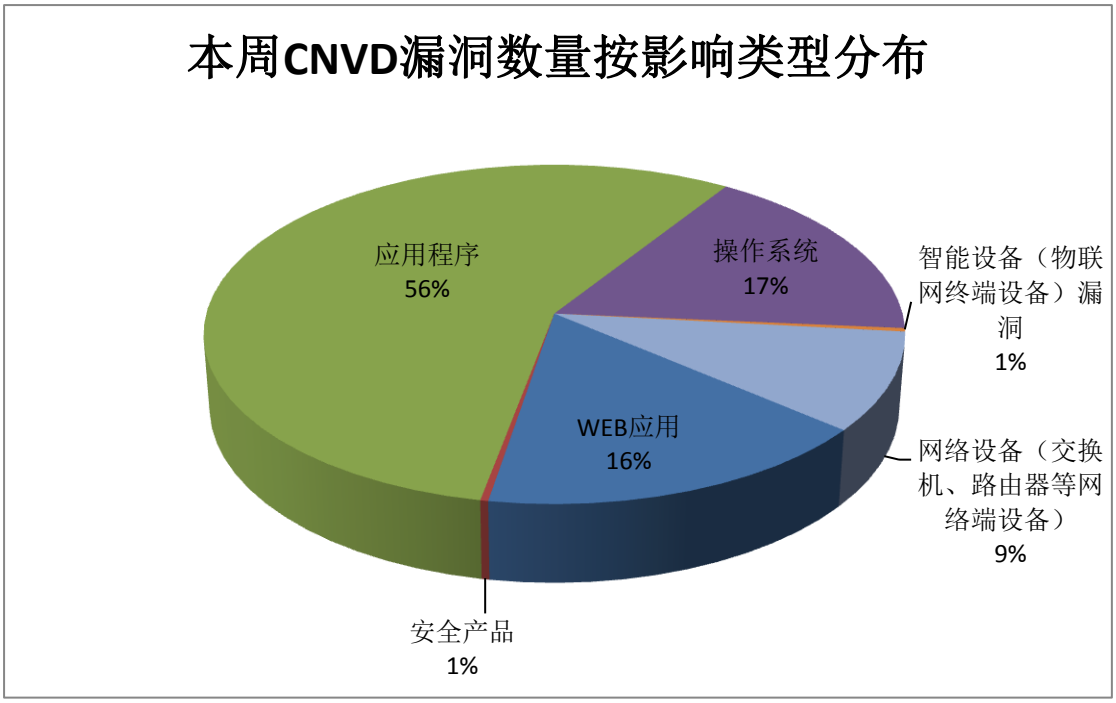

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、IBM 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	43	14%
2	Adobe	26	8%
3	IBM	19	6%
4	WordPress	19	6%
5	HP	17	6%
6	Wind River Systems	11	4%
7	Intel	6	2%
8	Linux	6	2%
9	Apache	5	2%
10	其他	156	50%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，4 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Verizon Wireless Fios Quantum Gateway（G1100）命令执行漏洞、多款 Huawei S 系列交换机输入验证错误漏洞、Dell Networking OS10 任意命令执行漏洞、WAGO Industrial Managed Switches 852-303、852-1305 和 852-1505 信任管理问题漏洞”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/

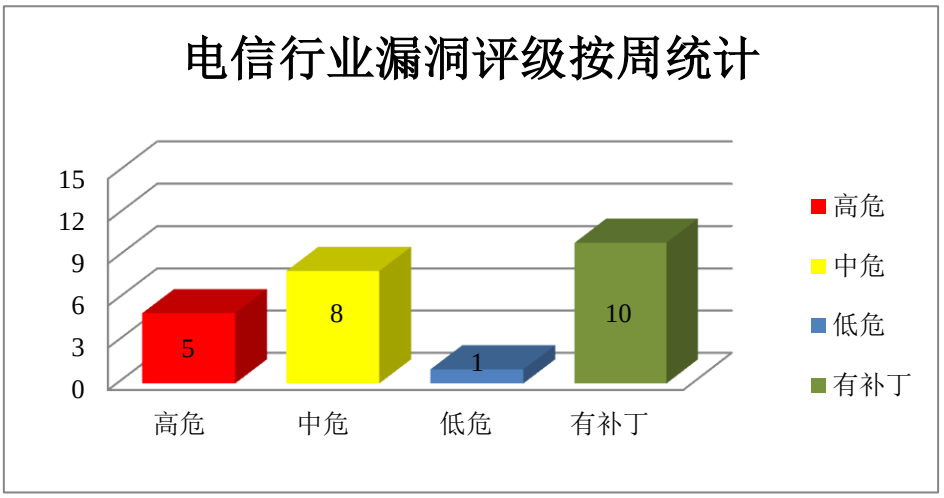

图 3 电信行业漏洞统计

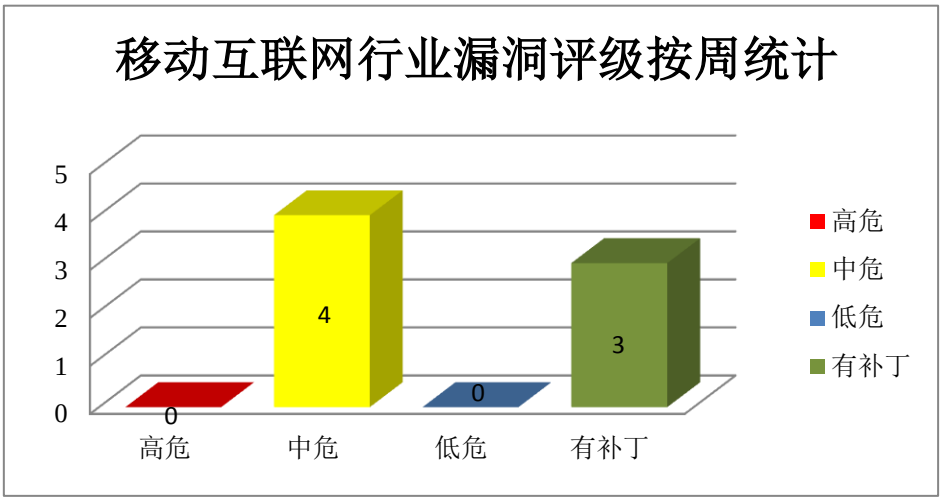

图 4 移动互联网行业漏洞统计

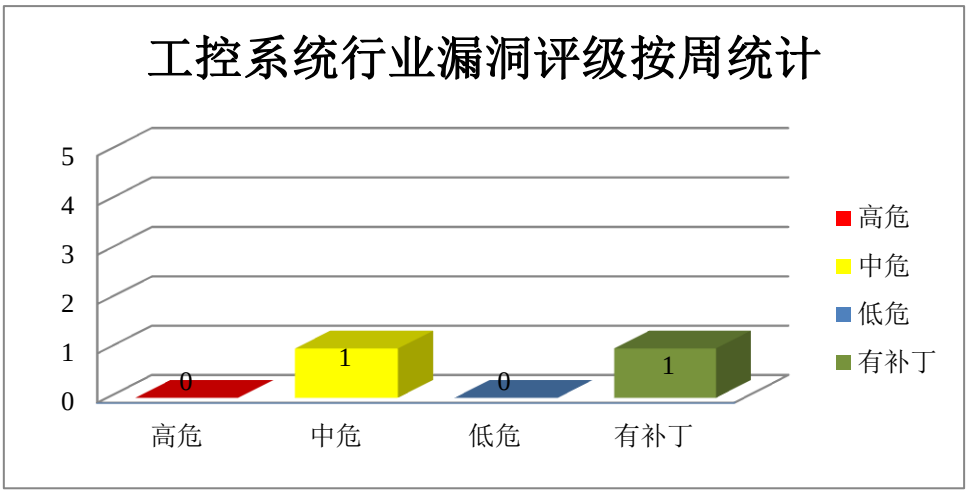

图 5 工控系统行业漏洞统计

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 Edge 是微软新的浏览器，从 EdgeHTML 内核迁移为 Chromium 内核，同时还会登陆到 Windows 7/8/8.1 和 macOS 平台。Internet Explorer 是微软公司推出的一款网页浏览器。本周，上述产品被披露存在远程内存破坏漏洞，攻击者可利用漏洞执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer Scripting Engine 远程内存破坏漏洞（CNVD-2019-24756、CNVD-2019-24757）、Microsoft Edge Chakra Scripting Engine 远程内存破坏漏洞（CNVD-2019-24840、CNVD-2019-24841、CNVD-2019-24842、CNVD-2019-24843、CNVD-2019-24844、CNVD-2019-24850）。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-2019-24756

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24757

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24840

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24841

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24842

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24843

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24844

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24850

2、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，该产品被披露存在越界读取漏洞，攻击者可利用漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 越界读取漏洞（CNVD-2019-24805、CNVD-2019-24806、CNVD-2019-24807、CNVD-2019-24808、CNVD-2019-24809、CNVD-2019-24810、CNVD-2019-24812、CNVD-2019-24811）。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-2019-24805

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24806

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24807

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24808

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24809

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24810

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24812

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24811

3、IBM 产品安全漏洞

IBM Cloud Private 是一套企业私有云解决方案。IBM Security Information Queue 是一款数据集成产品。IBM API Connect（APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM Cognos TM1 是一套用于规划、预算编制、预测和分析的企业规划软件。该软件可以快速地分析数据、对业务需求建模，并根据计划、预算和预测进行协作。IBM Daeja ViewONE Virtual 是一款基于 HTML5 的文档和图像查看器。IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Spectrum Control（前称 Tivoli Storage Productivity Center）是一套存储资源管理软件。本周，上述产品

被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，上传恶意文件，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Cloud Private Kubernetes API server 输入验证错误漏洞、IBM Security Information Queue 输入验证错误漏洞、IBM API Connect 信息泄露漏洞（CNVD-2019-25511）、IBM Cognos TM1 任意代码执行漏洞、IBM Daeja ViewONE Virtual 信息泄露漏洞、IBM Security Identity Manager 信息泄露漏洞（CNVD-2019-25734）、IBM Maximo Asset Management 文件上传漏洞、IBM Spectrum Control 信息泄露漏洞。其中，“IBM Cognos TM1 任意代码执行漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-25048
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25498
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25511
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25696
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25735
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25734
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25738
http://www.cnvd.org.cn/flaw/show/CNVD-2019-25743

4、HPE 产品安全漏洞

HPE Intelligent Management Center 是一套网络智能管理中心解决方案。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：HPE Intelligent Management Center 远程代码执行漏洞（CNVD-2019-24781、CNVD-2019-24782、CNVD-2019-24785、CNVD-2019-24783、CNVD-2019-24786、CNVD-2019-24787、CNVD-2019-24788、CNVD-2019-24789）。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-2019-24781
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24782
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24785
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24783
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24786
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24787
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24788
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24789

5、NETGEAR WNDR3400v3 栈缓冲区溢出漏洞

NETGEAR WNDR3400v3 是美国网件（NETGEAR）公司的一款无线路由器。本周，NETGEAR WNDR3400v3 被披露存在栈缓冲区溢出漏洞。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。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-2019-24852

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-2019-24558	Dell Networking OS10 任意命令执行漏洞	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.dell.com/support/article/us/en/04/sln316095
CNVD-2019-24766	Verizon Wireless Fios Quantum Gateway（G1100）命令执行漏洞	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://www.verizonwireless.com/
CNVD-2019-24769	Optergy Proton/Enterprise 任意代码执行漏洞	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://optergy.com/
CNVD-2019-24794	WordPress Simple Membership 插件跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wordpress.org/plugins/simple-membership/#developers
CNVD-2019-25064	Apache VCL SQL 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://lists.apache.org/thread.html/ffde9f87d0730ba6d4e1242eda56c1f1d6d0802ee4eda36fc1be3aaa@%3Cannounce.apache.org%3E
CNVD-2019-25065	Linux kernel 缓冲区溢出漏洞（CNVD-2019-25065）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=0926f91083f34d047abc74f1ca4fa6a9c161f7db
CNVD-2019-25516	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2019-25516）	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/mfsa2019-13/
CNVD-2019-25643	Lenovo Service Bridge 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://support.lenovo.com/us/zh/solutio

			ns/len-27725
CNVD-2019-25694	MATIO 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/tbeu/matio/releases/tag/v1.5.16
CNVD-2019-25731	Bitbucket Data Center migration tool 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://confluence.atlassian.com/bitbucketserver/bitbucket-server-security-advisory-2019-05-22-969526871.html

小结：本周，Microsoft 被披露存在远程内存破坏漏洞，攻击者可利用漏洞执行任意代码，发起拒绝服务攻击。此外，Adobe、IBM、HPE 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，上传恶意文件，执行任意代码等。NETGEAR WNDR3400v3 被披露存在栈缓冲区溢出漏洞。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。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、GetSimple CMS 远程代码执行漏洞

验证描述

GetSimple CMS 是一套使用 PHP 语言编写的内容管理系统（CMS）。

GetSimple CMS 3.3.15 及之前版本中存在远程代码执行漏洞。远程攻击者可利用该漏洞在受影响系统上执行任意的 PHP 代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/152961/GetSimpleCMS-3.3.15-Remote-Code-Execution.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-25044

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. StockX 遭黑客攻击，暴露了数百万用户记录

运动鞋交易平台 StockX 上周向用户发送一封密码重置的电子邮件，但并没有说明

原因。一位未透露姓名的数据卖家向媒体透露，黑客在 5 月份从网站上窃取了 680 多万条记录。卖家提供 1000 条数据样本，经证实这些信息确实是真实的。

参考链接：https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/

2. SanDisk SSD 仪表盘软件漏洞可导致数据丢失

用于管理 SanDisk 固态驱动器（SSD）的实用程序存在两个安全漏洞，可导致使用该应用程序的用户丢失数据。SanDisk 的 SSD 仪表板中的一个漏洞为攻击者提供了一种在运行该软件的系统上安装伪装成合法更新的恶意软件的方法，而实际上是传播勒索软件或银行特洛伊木马等恶意软件。

参考链接：https://www.darkreading.com/vulnerabilities---threats/flaws-in-sandisk-ssd-dashboard-present-malware-and-data-loss-risks/d/d-id/1335407?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

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