国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 06 月 10 日-2019 年 06 月 16 日 **2019 年第 24 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 293 个，其中高危漏洞 110 个、中危漏洞 162 个、低危漏洞 21 个。漏洞平均分值为 6.04。本周收录的漏洞中，涉及 0day 漏洞 185 个（占 63%），其中互联网上出现“RarmaRadio 'Server'拒绝服务漏洞、WordPress Antena_Ri Institute Themes 开放重定向漏洞”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 2883 个，与上周（1752 个）环比增长 65%。

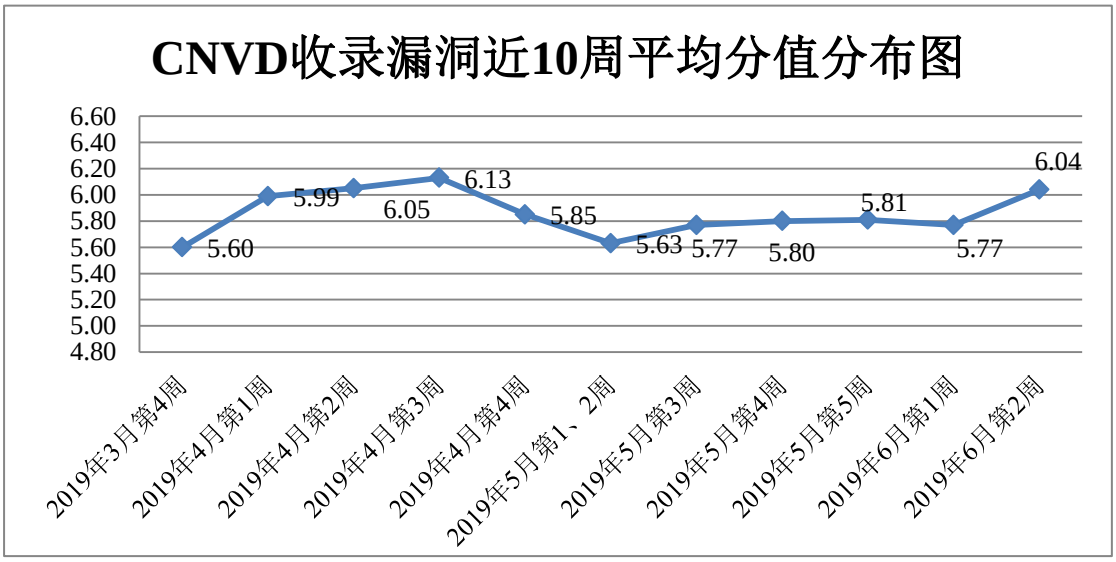

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 59 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 333 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 159 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：

石家庄开发区亿网科技发展有限公司、深圳市施瑞安科技有限公司、广东动易软件股份有限公司、成都鹏博士电信传媒集团股份有限公司、罗克韦尔自动化（中国）有限公司、重庆冰炫科技有限公司、北京金盘鹏图软件技术有限公司、山西先启科技有限公司、北京夜猫网络科技有限公司、新开普电子股份有限公司、长沙米拓信息技术有限公司、深圳市卓越迈创企业形象设计有限公司、北京通达信科科技有限公司、中国建材检验认证集团股份有限公司、浪潮集团有限公司、北京易知路科技有限公司、魔点科技、中国知网、卫生医药网、中国教育学会、中国担保协会、人民文学出版社版、GNU、Ollydbg、Notepad++、SemCms。

本周，CNVD 发布了《Microsoft 发布 2019 年 6 月安全更新》、《关于 Coremail 邮件系统存在配置信息泄露漏洞的安全公告》和《关于 Coremail 邮件系统存在服务未授权访问和服务接口参数注入漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5071

https://www.cnvd.org.cn/webinfo/show/5073

https://www.cnvd.org.cn/webinfo/show/5075

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、华为技术有限公司、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、上海银基信息安全技术股份有限公司、山东华鲁科技发展股份有限公司、任子行网络技术股份有限公司、内蒙古奥创科技有限公司、南京众智维信息科技有限公司、重庆贝特计算机系统工程有限公司、山东云天安全技术有限公司、广州锦行网络科技有限公司、北京信联科汇科技有限公司、杭州安信检测技术有限公司、新疆海狼科技有限公司、广州昊达信息科技有限公司、上海并擎软件科技有限公司、浙江鹏信信息科技股份有限公司、山石网科通信技术股份有限公司、河南信安世纪科技有限公司、江苏天网计算机技术有限公司、四川无国界信息技术有限公司及其他个人白帽子向 CNVD 提交了 2209 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 1413 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）	1016	1016
奇安信网神（补天平台）	397	397
北京天融信网络安全技术有限公司	258	1
哈尔滨安天科技集团股份有限公司	215	0
新华三技术有限公司	158	2
华为技术有限公司	148	0
深信服科技股份有限公司	130	0
北京神州绿盟科技有限公司	77	3
中国电信集团系统集成有限责任公司	69	0
恒安嘉新(北京)科技股份公司	62	0
北京启明星辰信息安全技术有限公司	51	2
北京数字观星科技有限公司	38	0
厦门服云信息科技有限公司	12	0
中新网络信息安全股份有限公司	12	12
北京知道创宇信息技术股份有限公司	4	4
南京联成科技发展股份有限公司	4	4
沈阳东软系统集成工程有限公司	1	1
国瑞数码零点实验室	771	771
上海银基信息安全技术股份有限公司	53	53
山东华鲁科技发展股份有限公司	48	48
任子行网络技术股份有限公司	34	34
内蒙古奥创科技有限公司	24	24

南京众智维信息科技有限公司	15	15
重庆贝特计算机系统工程有限公司	12	12
山东云天安全技术有限公司	10	10
广州锦行网络科技有限公司	6	6
北京信联科汇科技有限公司	3	3
杭州安信检测技术有限公司	3	3
新疆海狼科技有限公司	3	3
广州昊达信息科技有限公司	2	2
上海并擎软件科技有限公司	2	2
浙江鹏信信息科技股份有限公司	2	2
山石网科通信技术股份有限公司	1	1
河南信安世纪科技有限公司	1	1
江苏天网计算机技术有限公司	1	1
四川无国界信息技术有限公司	1	1
CNCERT 天津分中心	29	29
CNCERT 河北分中心	5	5
CNCERT 贵州分中心	4	4
CNCERT 海南分中心	4	4
CNCERT 西藏分中心	3	3
CNCERT 青海分中心	2	2
CNCERT 广西分中心	1	1
个人	401	401

报送总计	4093	2883

本周漏洞按类型和厂商统计

本周，CNVD 收录了 293 个漏洞。应用程序 158 个，WEB 应用 106 个，网络设备（交换机、路由器等网络端设备）11 个，安全产品 8 个，操作系统 5 个，智能设备（物联网终端设备）漏洞 4 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	158
WEB 应用	106
网络设备（交换机、路由器等网络端设备）	11
安全产品	8
操作系统	5
智能设备（物联网终端设备）漏洞	4
数据库	1

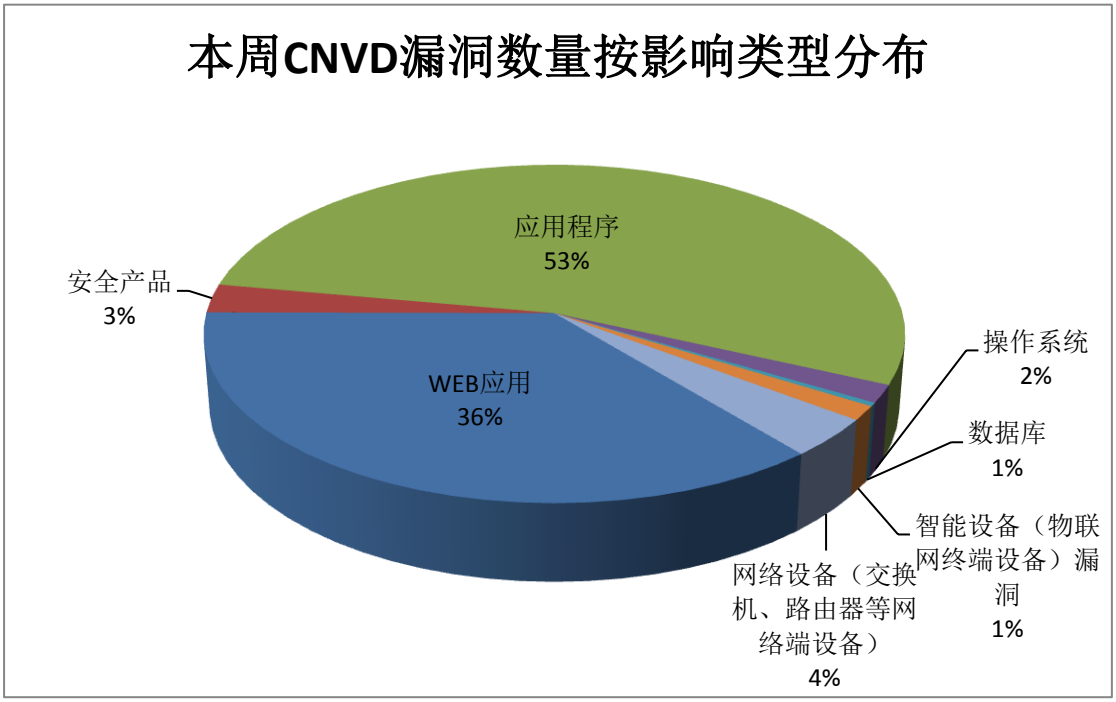

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、福州凌夕网络科技有限公司、深圳搜豹网络有限公司等多家厂商的产品，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	Mozilla	18	6%
2	福州凌夕网络科技有限公司	12	4%
3	深圳搜豹网络有限公司	12	4%
4	Moxa	11	4%
5	SIEMENS	10	4%
6	Google	9	3%
7	Microsoft	9	3%
8	Xpdf	6	2%
9	IBM	6	2%
10	其他	200	68%

本周行业漏洞收录情况

本周，CNVD 收录了 3 个电信行业漏洞，9 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Siemens LOGO!8 授权问题漏洞、Siemens LOGO!8 缓冲区溢出漏洞、Siemens LOGO!8 BM 访问控制错误漏洞”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/

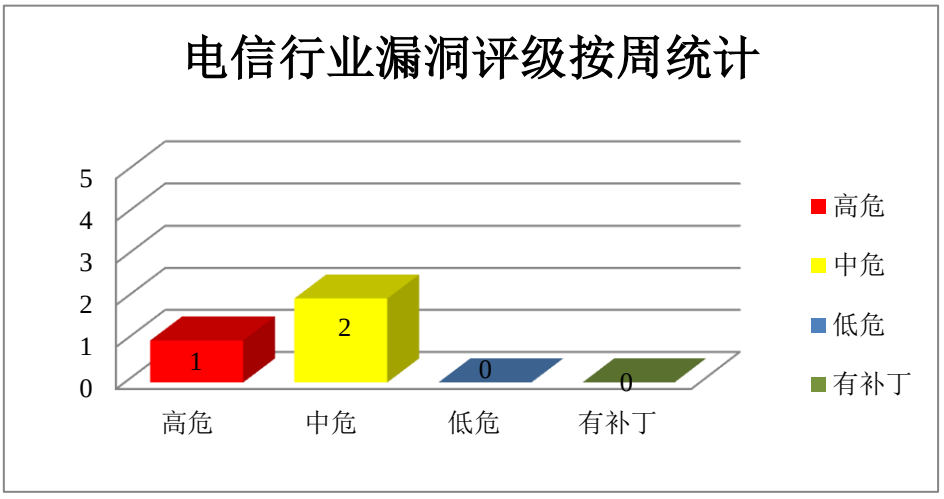

图 3 电信行业漏洞统计

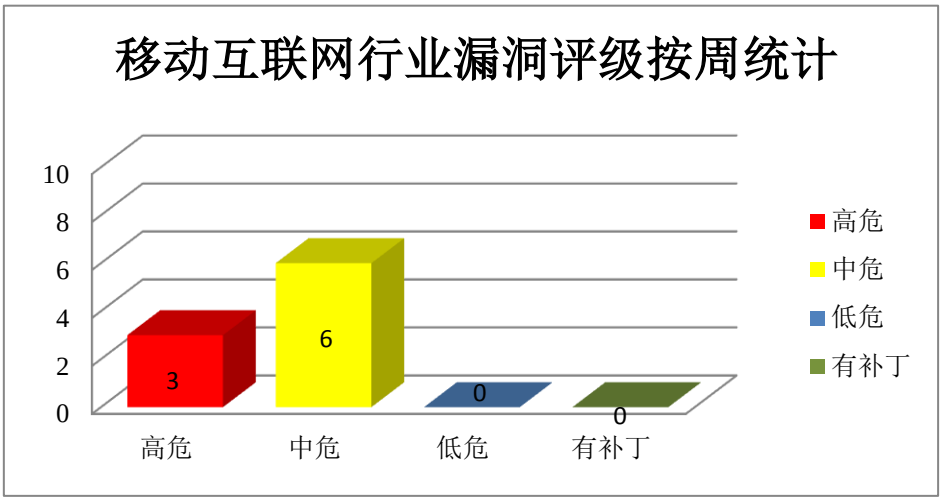

图 4 移动互联网行业漏洞统计

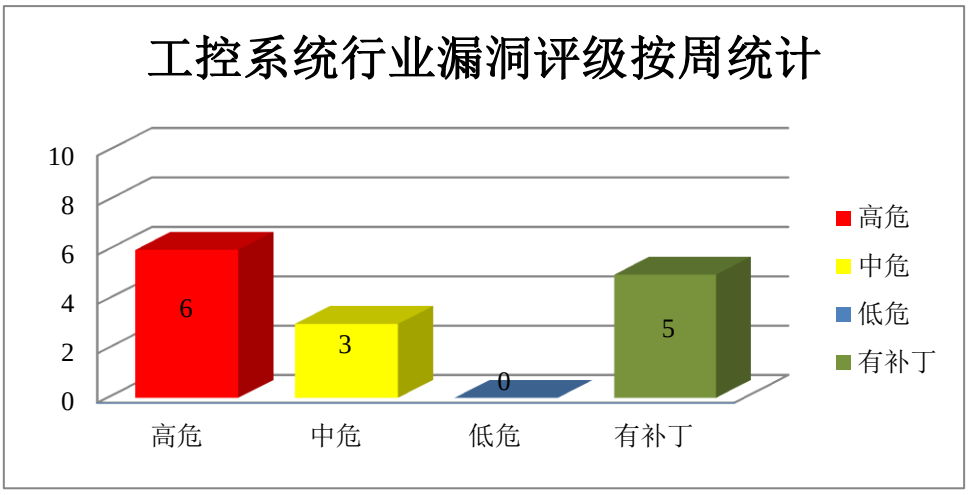

图 5 工控系统行业漏洞统计

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、Coremail 邮件系统存在配置信息泄露漏洞

Coremail 邮件系统是论客科技（广州）有限公司（以下简称论客公司）自主研发的大型企业邮件系统，为客户提供电子邮件整体技术解决方案及企业邮局运营服务。Coremail 论客邮件系统被披露存在信息泄露漏洞。攻击者可利用该漏洞获取敏感信息。目前，厂商已经发布了漏洞的修补程序。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-2019-16798

2、Coremail 邮件系统存在服务未授权访问和服务接口参数注入漏洞

Coremail 邮件系统是论客科技（广州）有限公司（以下简称论客公司）自主研发的大型企业邮件系统，为客户提供电子邮件整体技术解决方案及企业邮局运营服务。Cor

email 邮件系统被披露存在服务未授权访问和服务接口参数注入漏洞。攻击者可利用漏洞在未授权的情况下访问部分服务接口和进行接口参数注入操作。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/webinfo/show/5075

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。本周，上述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，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：Mozilla Firefox 和 Mozilla Firefox ESR 定时攻击漏洞、Mozilla Firefox 和 Mozilla Firefox ESR XMLHttpRequest 内存错误引用漏洞、Mozilla Firefox 和 Mozilla Firefox ESR crash generation server 资源管理错误漏洞、Mozilla Firefox 和 Mozilla Firefox ESR 内存破坏漏洞、Mozilla Firefox 和 Mozilla Firefox ESR 内存错误引用漏洞、Mozilla Firefox 和 Mozilla Firefox ESR 类型混淆漏洞、Mozilla Firefox 内存错误引用漏洞（CNVD-2019-17486）、Mozilla Firefox 命令执行漏洞。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-16994
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16993
http://www.cnvd.org.cn/flaw/show/CNVD-2019-16995
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17474
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17476
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17475
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17486
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17485

4、Siemens 产品安全漏洞

Siemens Siveillance VMS 是一套监控视频管理软件。LOGO!8 是西门子第 8 代智能逻辑控制器，是西门子 PLC 家族里的 Nano PLC，它简化了编程组态，集成的面板可显示更多的内容，并可通过集成的以太网接口轻松组网高效互联。Siemens LOGO! Soft Comfort 是一个工程软件。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，绕过安全限制，获取系统的未授权访问权限，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Google Chrome Swiftshader 缓冲区溢出漏洞（CNVD-2019-17139）、Google Chrome Download Manager 内存错误引用漏洞、Google Chrome Blink 安全绕过漏洞（CNVD-2019-17513）、Google Chrome 安全绕过漏洞（CNVD-2019-17515）、Google Chrome Extensions 安全绕过漏洞（CNVD-2019-17514）、Google Chrome 敏感信息泄露漏洞（CNVD-2019-17516）、Google Chrome V8 安全绕过漏洞、G

oogle Chrome 安全绕过漏洞（CNVD-2019-17517）。其中，“Google Chrome Download Manager 内存错误引用漏洞”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-2019-17146

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17147

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17148

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17150

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17151

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17520

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17519

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17522

5、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，造成内存破坏。

CNVD 收录的相关漏洞包括：Microsoft Edge 和 ChakraCore 缓冲区溢出漏洞（CNVD-2019-16511）、Microsoft Windows GDI 远程代码执行漏洞（CNVD-2019-16510）、Microsoft ChakraCore 和 Microsoft Edge 远程代码执行漏洞（CNVD-2019-16745、CNVD-2019-16746、CNVD-2019-16748）、Microsoft Edge 远程代码执行漏洞（CNVD-2019-16747）、Microsoft Edge 和 ChakraCore 远程代码执行漏洞（CNVD-2019-16749）、多款 Microsoft 产品远程代码执行漏洞（CNVD-2019-16750）。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-2019-17139

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17498

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17513

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17515

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17514

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17516

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17518

http://www.cnvd.org.cn/flaw/show/CNVD-2019-17517

6、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。Windows Jet Database Engine 是其中的一个数据库引擎。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Internet Explorer 是一款 Windows 操作系统附带的 Web 浏览器。本周，该产品被披露存在多个漏

洞，攻击者可利用漏洞绕过 NTLM MIC 保护，执行任意代码，造成内存破坏等。

CNVD 收录的相关漏洞包括：Microsoft Windows NTLM 篡改安全绕过漏洞、Microsoft Windows Jet Database Engine 缓冲区溢出漏洞（CNVD-2019-17523、CNVD-2019-17525、CNVD-2019-17524）、Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-17527、CNVD-2019-17528）、Microsoft Edge 和 Internet Explorer 缓冲区溢出漏洞（CNVD-2019-17529）。其中，除“Microsoft Windows NTLM 篡改安全绕过漏洞”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-2019-17130
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17523
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17525
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17524
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17526
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17527
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17528
http://www.cnvd.org.cn/flaw/show/CNVD-2019-17529

7、D-Link DIR-818LW 命令注入漏洞

D-Link DIR-818LW 是一款无线路由器。D-Link DIR-818LW 被披露存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。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-2019-17125

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-2019-16840	Cisco Industrial Network Director 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190605-ind-rce
CNVD-2019-16943	HPE Intelligent Management Center (IMC)路径遍历漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.hpe.com/hpesc/public/home
CNVD-201	SalesAgility SuiteCRM SQL	高	厂商已发布了漏洞修复程序，请及时

9-16999	注入漏洞		关注更新：https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_5
CNVD-2019-17127	ZOHO ManageEngine Netflow Analyzer SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.manageengine.com/products/netflow/readme.html#124029
CNVD-2019-17131	Sitecore Experience Platform 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://dev.sitecore.net/Downloads/Sitecore%20Experience%20Platform/91/Sitecore%20Experience%20Platform%2091%20Update1/Release%20Notes
CNVD-2019-17309	Vim 和 Neovim 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/vim/vim/commit/53575521406739cf20bbe4e384d88e7dca11f040
CNVD-2019-17312	Prima Systems FlexAir 脚本上传执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://primasystems.eu/
CNVD-2019-17313	HPE Integrated Lights-Out 跨站脚本漏洞	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.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03917en_us
CNVD-2019-17316	aubio 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://github.com/aubio/aubio/blob/0.4.9/ChangeLog
CNVD-2019-17321	HotelDruid SQL 注入漏洞	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：http://www.hoteldruid.com/

小结：本周，Mozilla 被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，执行任意代码，发起拒绝服务攻击等。此外，Siemens、Google、Microsoft 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，绕过安全限制，获取系统的未授权访问权限，执行任意代码，造成内存破坏等。D-Link DIR-818LW 被披露存在命令注入漏洞。攻击者可利用该漏洞执行非法命令。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、RarmaRadio 'Server'拒绝服务漏洞

验证描述

RarmaRadio 是一款免费的网络收音机软件。

RarmaRadio 'Server'存在拒绝服务漏洞。攻击者可利用漏洞发起拒绝服务攻击。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=33297

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-16759

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. 印象笔记扩展被曝严重漏洞，可泄露数百万用户的敏感信息

6 月 13 日，印象笔记 Web Clipper Chrome 扩展中被曝存在一个严重缺陷，可导致潜在攻击者访问用户存储在第三方网络服务中的敏感信息。该问题是一个全局跨站点脚本(UXSS)漏洞，编号为 CVE-2019-12592，源自一个印象笔记 Web Clipper 逻辑编程错误，使其可能绕过浏览器的同源策略，导致攻击者能够在印象笔记域名以外的内联框架中获得代码执行权限。发现该漏洞的安全公司 Guardio 表示，“由于印象笔记广为流行，该问题可能影响使用该扩展的客户和企业，在发现之时它的用户量为 460 万左右。”

参考链接：https://www.freebuf.com/news/205965.html

2. Telegram 服务器遭 DDoS 攻击，服务中断

近日，Telegram 服务器遭到针对性的分布式拒绝服务攻击导致服务中断，主要影响南美和北美的用户，其他地区也出现了连接缓慢的情况。在 Twitter 的一则声明中，Telegram 表示僵尸网络向 Telegram 服务器发送了庞大无用流量，服务器无法再处理来自合法用户的请求，从而导致连接不稳定。根据 Downdetector（一个实时跟踪影响各种数字服务的中断的网站）的数据，DDoS 攻击影响的热点是美洲东海岸、英国、荷兰、德国、乌克兰、俄罗斯和中国。

参考链接：https://www.bleepingcomputer.com/news/security/ddos-attack-on-telegram-messenger-leaves-users-hanging/

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