国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 12 月 31 日-2019 年 01 月 06 日 **2019 年第 1 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 138 个，其中高危漏洞 44 个、中危漏洞 78 个、低危漏洞 16 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 75 个（占 54%），其中互联网上出现“TP-Link Archer C5 远程命令执行漏洞、WordPress 插件 Audio Record 任意文件上传漏洞”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 1496 个，与上周（1657 个）环比下降 10%。

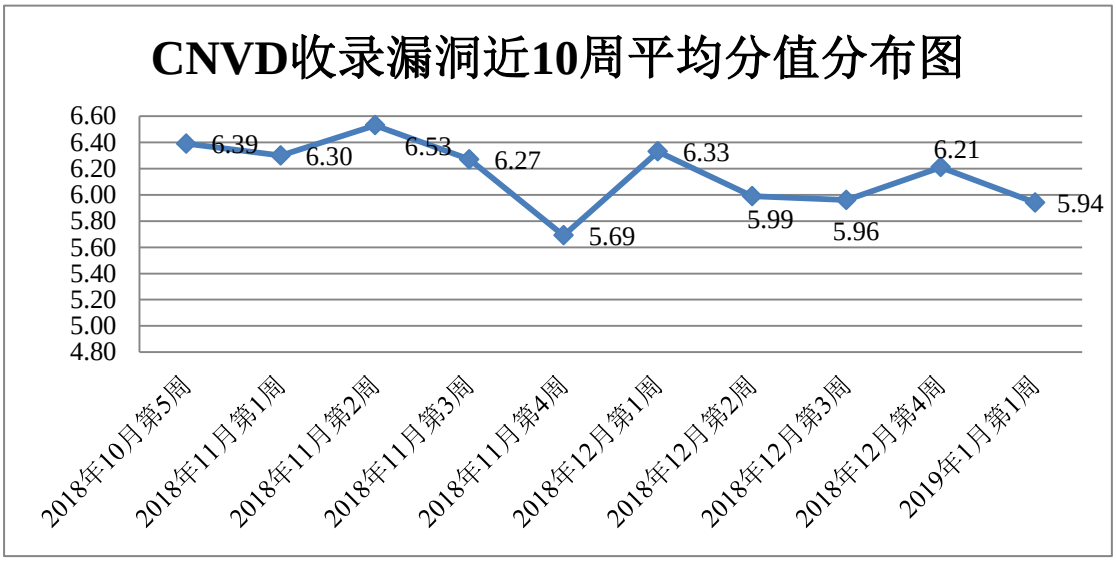

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 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 190 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 98 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16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：

淄博闪灵网络科技有限公司、北京飞锐科技有限公司、上海丹帆网络科技有限公司、贵州道坦坦科技股份有限公司、江苏金智教育信息股份有限公司、得实信息科技有限公司、南阳市宛都科技有限公司、西安格创网络科技有限公司、上海思锐信息技术有限公司、山西牛酷信息科技有限公司、山东潍微科技股份有限公司、上海安为信息技术有限公司、广州坚和网络科技有限公司、中国中央广播电视总台、玉溪市气象局、森动网、华夏化工网、HTML5VideoPlayer.net、Oracle、zzzcms。

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、北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、北京数字观星科技有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。天津市国瑞数码安全系统股份有限公司、安徽锋刃信息科技有限公司、中新网络信息安全股份有限公司、山东云天安全技术有限公司、任子行网络技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京国舜科技股份有限公司、河南信安世纪科技有限公司、新疆海狼科技有限公司、山石网科通信技术有限公司、江苏百达智慧网络科技有限公司（含光实验室）及其他个人白帽子向 CNVD 提交了 1496 个以事件型漏洞为主的原创漏洞，其中包括 360 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 1099 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）	713	713
360 网神（补天平台）	386	386
哈尔滨安天科技集团股份有限公司	174	0
北京天融信网络安全技术有限公司	149	1
北京启明星辰信息安全技术有限公司	103	0
北京数字观星科技有限公司	89	0
华为技术有限公司	85	0

中国电信集团系统集成有限责任公司	55	5
北京神州绿盟科技有限公司	51	0
新华三技术有限公司	50	0
深信服科技股份有限公司	17	0
恒安嘉新(北京)科技股份公司	12	0
厦门服云信息科技有限公司	5	0
天津市国瑞数码安全系统股份有限公司	100	100
安徽锋刃信息科技有限公司	48	48
中新网络信息安全股份有限公司	43	43
山东云天安全技术有限公司	19	19
任子行网络技术股份有限公司	17	17
远江盛邦（北京）网络安全科技股份有限公司	12	12
北京国舜科技股份有限公司	7	7
河南信安世纪科技有限公司	3	3
新疆海狼科技有限公司	3	3
山石网科通信技术有限公司	1	1
江苏百达智慧网络科技有限公司（含光实验室）	1	1
个人	137	137
报送总计	2280	1496

本周漏洞按类型和厂商统计

本周，CNVD 收录了 138 个漏洞。应用程序漏洞 54 个，WEB 应用漏洞 51 个，操作系统漏洞 22 个，网络设备漏洞 10 个，安全产品漏洞 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
应用程序漏洞	54
WEB 应用漏洞	51
操作系统漏洞	22
网络设备漏洞	10
安全产品漏洞	1

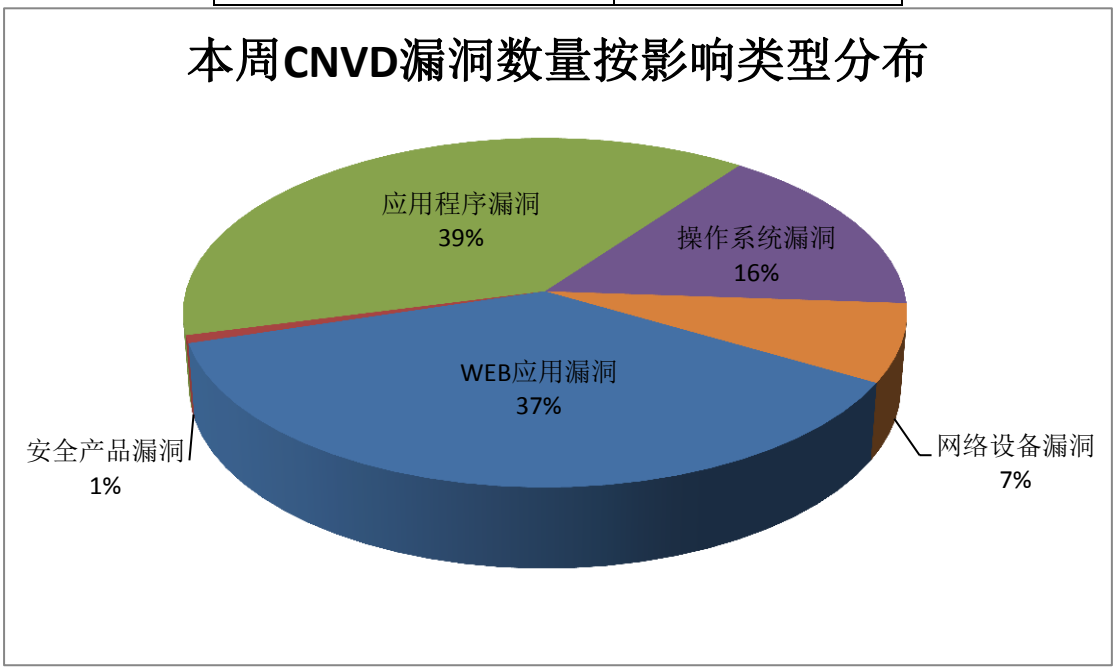

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Cisco、Google 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	14	10%
2	Cisco	10	7%
3	Google	10	7%
4	SugarCRM	8	6%
5	WordPress	8	6%
6	Cagintranet Networks	3	2%
7	Gnuplot	3	2%
8	PHPMyWind	3	2%
9	Red Hat	3	2%
10	其他	76	56%

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，1 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，“Cisco Small Business Switches 身份验证绕过漏洞”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/

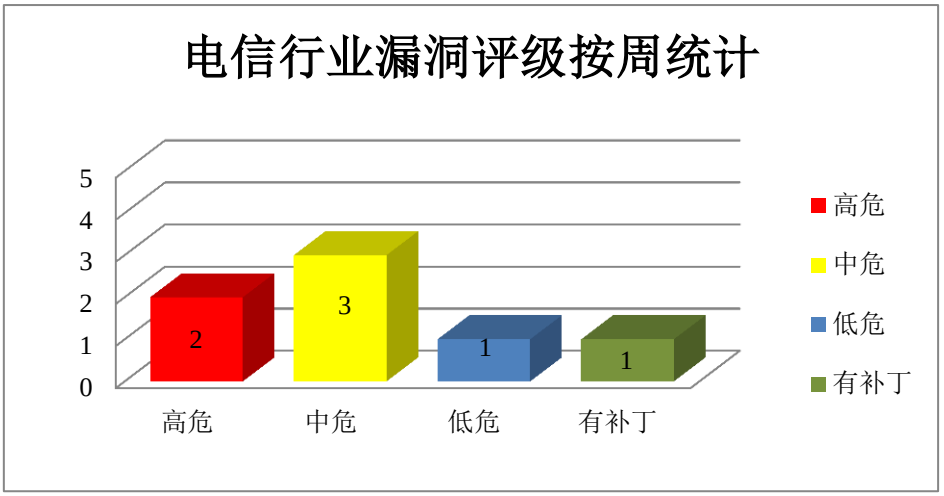

图 3 电信行业漏洞统计

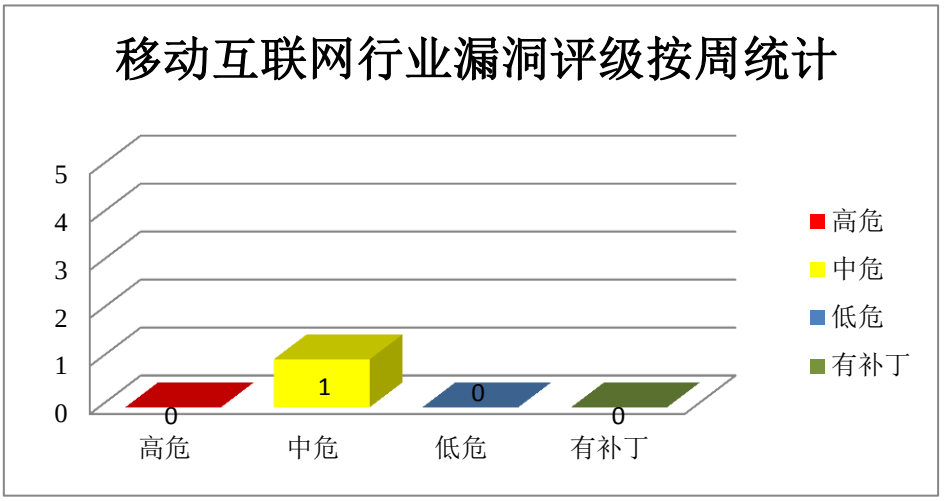

图 4 移动互联网行业漏洞统计

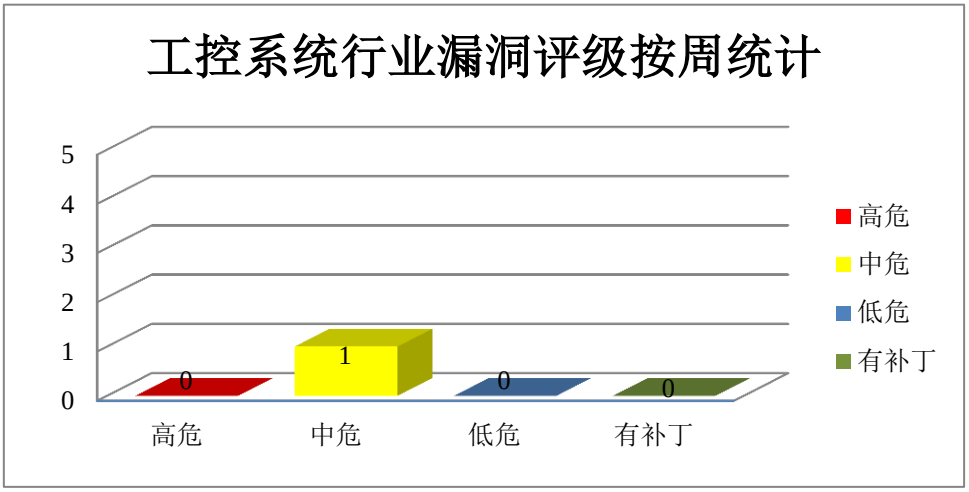

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是一款 Web 浏览器，是 Windows 操作系统附带的默认浏览器。Microsoft Windows Server 2019、Windows 10 等都是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft Windows 7 SP1 是一套个人电脑使用的操作系统。Windows Server 2008 R2 SP1 是一套服务器使用的操作系统。Microsoft .NET Framework 是编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。Open Data Protocol （开放数据协议，OData）是用来查询和更新数据的一种 Web 协议，其提供了把存在于应用程序中的数据暴露出来的方式，该标准由微软发起。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，提升权限，执行任意代码，破坏内存，导致拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 脚本引擎远程代码执行漏洞、Microsoft Windows 本地权限提升漏洞（CNVD-2019-00337）、Microsoft Windows SMB 服务器信息泄露漏洞、Microsoft Windows SMB 服务器拒绝服务漏洞、Microsoft .NET Framework 远程执行代码漏洞、Microsoft Jet Database Engine 缓冲区溢出漏洞（CNVD-2019-00354）、Microsoft OData 拒绝服务漏洞、Microsoft Windows GDI Component 信息泄露漏洞。其中，“Microsoft Internet Explorer 脚本引擎远程代码执行漏洞、Microsoft Windows SMB 服务器拒绝服务漏洞、Microsoft .NET Framework 远程执行代码漏洞、Microsoft Jet Database Engine 缓冲区溢出漏洞（CNVD-2019-00354）”的综合评级为为“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-2019-00243

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00337
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00349
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00351
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00353
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00354
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00359
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00357

2、Cisco 产品安全漏洞

Cisco Adaptive Security Appliances（ASA，自适应安全设备）Software 是一套运行于防火墙中的操作系统。Cisco Prime Collaboration Assurance（PCA）是一套企业协作网络管理解决方案。Cisco Energy Management Suite（CEMS）是一套能源管理套件。Cisco Video Surveillance Media Server 是一套监控视频管理解决方案。Cisco Firepower System Software 是一款下一代防火墙产品（NGFW）。Cisco Small Business 200 Series Smart Switches 是小型智能交换机设备。Small Business Switches Software 是一套运行在其中的交换机软件。Cisco Content Security Management Appliance（SMA）是一套内容安全管理设备。Cisco Energy Management Suite 是一套能源管理套件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取和写入信息，执行未授权操作，提升权限，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliances Software authorization 子系统远程权限提升漏洞、Cisco Prime Collaboration Assurance 任意文件覆盖漏洞、Cisco Energy Management Suite 访问绕过漏洞、Cisco Video Surveillance Media Server 拒绝服务漏洞、Cisco Firepower System Software 安全绕过漏洞（CNVD-2019-00344）、Cisco Small Business Switches 身份验证绕过漏洞、Cisco Content Security Management Appliance 跨站脚本漏洞、Cisco Energy Management Suite XML 外部实体注入漏洞。其中，“Cisco Adaptive Security Appliances Software authorization 子系统远程权限提升漏洞、Cisco Small Business Switches 身份验证绕过漏洞、Cisco Energy Management Suite XML 外部实体注入漏洞”的综合评级为为“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-2019-00338
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00342
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00340
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00345
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00344
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00343

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00347

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00346

3、Google 产品安全漏洞

Android 是美国谷歌（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权限提升和缓冲区溢出漏洞，攻击者可利用漏洞提升权限，造成拒绝服务或执行代码。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件权限提升漏洞（CNVD-2019-00122、CNVD-2019-00123）、Google Android Qualcomm 组件缓冲区溢出漏洞（CNVD-2019-00124、CNVD-2019-00125、CNVD-2019-00127）、Google Android Kernel 组件权限提升漏洞（CNVD-2019-00129、CNVD-2019-00130、CNVD-2019-00131）。上述漏洞的综合评级为为“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-2019-00122

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00123

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00124

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00125

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00127

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00129

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00130

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00131

4、SugarCRM 品安全漏洞

SugarCRM 是一套开源的客户关系管理系统（CRM）。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞从数据库中读取敏感数据，注入和执行任意的 PHP 代码等。

CNVD 收录的相关漏洞包括：SugarCRM (WorkFlow module) PHP 代码注入漏洞、SugarCRM (WorkFlow module) PHP 代码注入漏洞、SugarCRM (portal_get_related_notes) SQL 注入漏洞、SugarCRM (Web Logic Hooks module) PHP 代码注入漏洞、SugarCRM (ConnectorsController)服务器端请求伪造漏洞、SugarCRM (SaveDropDown) PHP 代码注入漏洞、SugarCRM (Web Logic Hooks module)路径遍历漏洞、SugarCRM (addLabels) PHP 代码注入漏洞。其中，“SugarCRM (portal_get_related_notes) SQL 注入漏洞”的综合评级为为“高危”。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-2019-00132

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00220

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00221

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00222

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00223

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00225

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00227

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00228

5、Linux kernel 拒绝服务漏洞（CNVD-2019-00366）

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。本周，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成系统崩溃。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-2019-00366

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-2019-00126	Google Android Kernel 组件权限提升漏洞（CNVD-2019-00126）	高	厂商已发布漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/pixel/2018-08-01
CNVD-2019-00133	CuppaCMS 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/CuppaCMS/CuppaCMS
CNVD-2019-00130	Google Android Kernel 组件权限提升漏洞（CNVD-2019-00130）	高	厂商已发布漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/pixel/2018-08-01
CNVD-2019-00328	Contiki-NG 缓冲区溢出漏洞（CNVD-2019-00328）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/contiki-ng/contiki-ng/pull/702/files
CNVD-2019-00346	Cisco Energy Management Suite XML 外部实体注入漏洞	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-20181107-ems-xml-xxe
CNVD-2019-00351	Microsoft Windows SMB 服务器拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8335
CNVD-201	Apache NetBeans 远程命令执	高	目前厂商已发布升级补丁以修复漏

9-00360	行漏洞		洞，补丁获取链接：https://lists.apache.org/thread.html/d1c37966a316a326ab4ff4d4bc056322e8adcbe984e8145c0ecda7fa@%3Cdev.netbeans.apache.org%3E
CNVD-2019-00361	Dolibarr SQL 注入漏洞（CNVD-2019-00361）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/850b939ffd2c7a4443649331b923d5e0da2d6446
CNVD-2019-00364	IBM API Connect 提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10792055
CNVD-2019-00367	Plikli CMS 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://www.plikli.com/

小结：本周，Microsoft 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，破坏内存，导致拒绝服务。此外，Cisco、Google、SugarCRM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞从数据库中读取敏感数据，执行未授权操作，提升权限，造成拒绝服务或执行代码等。另外，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成系统崩溃。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 插件 Audio Record 任意文件上传漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 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。

WordPress 插件 Audio Record 存在任意文件上传漏洞。允许攻击者上传 webshell，获得服务器权限。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=31835

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-00229

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. Mac 工具 CleanMyMac X 被曝存在多个权限提升漏洞

近日，思科 Talos 公布了 MacPaw 的 CleanMyMac X 软件中的一大批漏洞。CleanMyMac X 是 Mac 操作系统的清理应用程序，允许用户通过扫描未使用或不必要的文件并删除它们来释放机器上的额外空间。这些错误允许攻击者访问受害者本计算机，以 root 权限修改文件系统。根据协调披露政策，Cisco Talos 与 MacPaw 合作确保解决这些问题并为受影响的客户提供更新。厂商建议用户更新到该软件的最新版本（CleanMyMac X 版本 4.2.0）。有几种方法可以让攻击者绕过通常的保护措施来获取对机器的更大访问权限并以 root 身份修改文件系统。

参考链接：https://blog.talosintelligence.com/2019/01/vulnerability-spotlight-CleanMyMac-X.html#more

2. Windows 0day 任意文件读取漏洞

近日，国外安全研究员又一次在推特上公布了新的 Windows 0 day 漏洞。该漏洞是由于当调用 MsiAdvertiseProduct 这个函数时会导致 windows 安装服务复制一个文件，在复制文件时我们可以通过 TOCTOU 的攻击方式控制传进 MsiAdvertiseProductA 的第一个参数，将该参数在检查通过后被替换成我们实际需要读取的文件，达到越权的效果。允许低权限用户或恶意程序读取目标 Windows 主机上任意文件的内容，但不可对文件进行写入操作。

参考链接：https://www.freebuf.com/vuls/192876.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