

信息安全漏洞周报

2017 年 11 月 06 日-2017 年 11 月 12 日

2017 年第 46 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 534 个，其中高危漏洞 153 个、中危漏洞 333 个、低危漏洞 48 个。漏洞平均分为 5.93。本周收录的漏洞中，涉及 0day 漏洞 71 个（占 13%），其中互联网上出现“iTech Gigs Script SQL 注入漏洞、Vastal I-Tech Agent Zone SQL 注入漏洞”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 638 个，与上周（832 个）环比下降 23%。

CNVD收录漏洞近10周平均分分布图

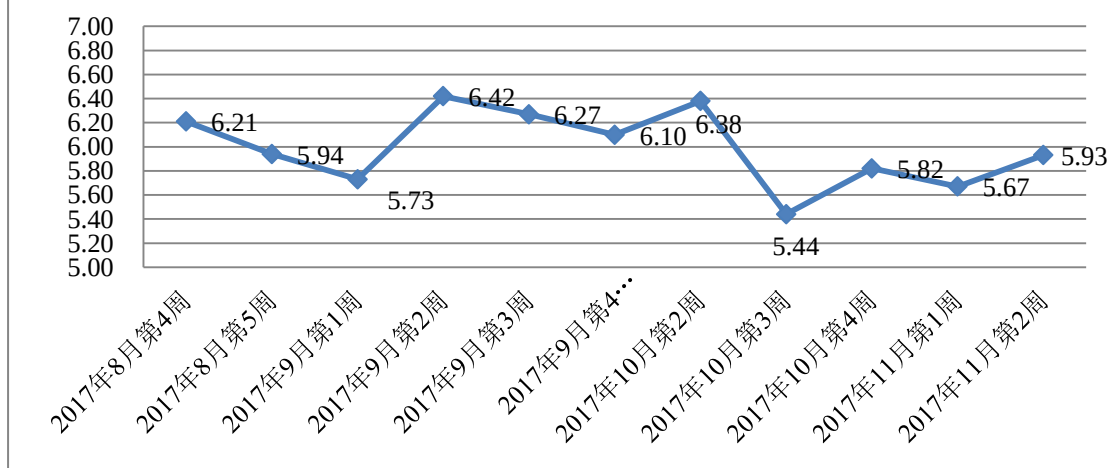


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、H3C、安天实验室、天融信、恒安嘉新等单位报送数量较多。深圳市鼎安天下信息科技有限公司、四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、南京联成科技发展股份有

限公司君立华域、福建榕基软件股份有限公司、安元实验室、广州万方计算机科技有限公司、网信智安、福建省海峡信息技术公司及其他个人白帽子向 CNVD 提交了 638 个以事件型漏洞为主的原创漏洞。

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
H3C	225	0
天融信	210	5
安天实验室	206	0
360 网神	178	178
华为技术有限公司	157	0
恒安嘉新	115	0
漏洞盒子	113	113
杭州安恒信息技术有限公司	44	0
北京数字观星科技有限公司	41	0
中国电信集团系统集成有限责任公司	34	0
绿盟科技	29	0
知道创宇	1	0
南京铨迅信息技术股份有限公司	1	1
四川虹微技术有限公司 (子午攻防实验室)	14	14
中新网络信息安全股份有限公司	11	11
南京联成科技发展股份有限公司	4	4
深圳市鼎安天下信息科技有限公司	3	3
福建省海峡信息技术公司	3	3
上海观安信息技术股份有限公司	2	2

福建榕基软件股份有限公司	2	2
北京智游网安科技有限公司	1	1
君立华域	3	3
CNCERT 山西分中心	11	11
CNCERT 广东分中心	2	2
CNCERT 吉林分中心	1	1
个人	284	284
报送总计	1695	638



本周漏洞按类型和厂商统计

本周，CNVD 收录了 534 个漏洞。其中应用程序漏洞 317 个，操作系统漏洞 95 个，网络设备漏洞 62 个，web 应用漏洞 52 个，数据库漏洞 5 个，安全产品漏洞 3 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	317
操作系统漏洞	95
网络设备漏洞	62
web 应用漏洞	52
数据库漏洞	5
安全产品漏洞	3

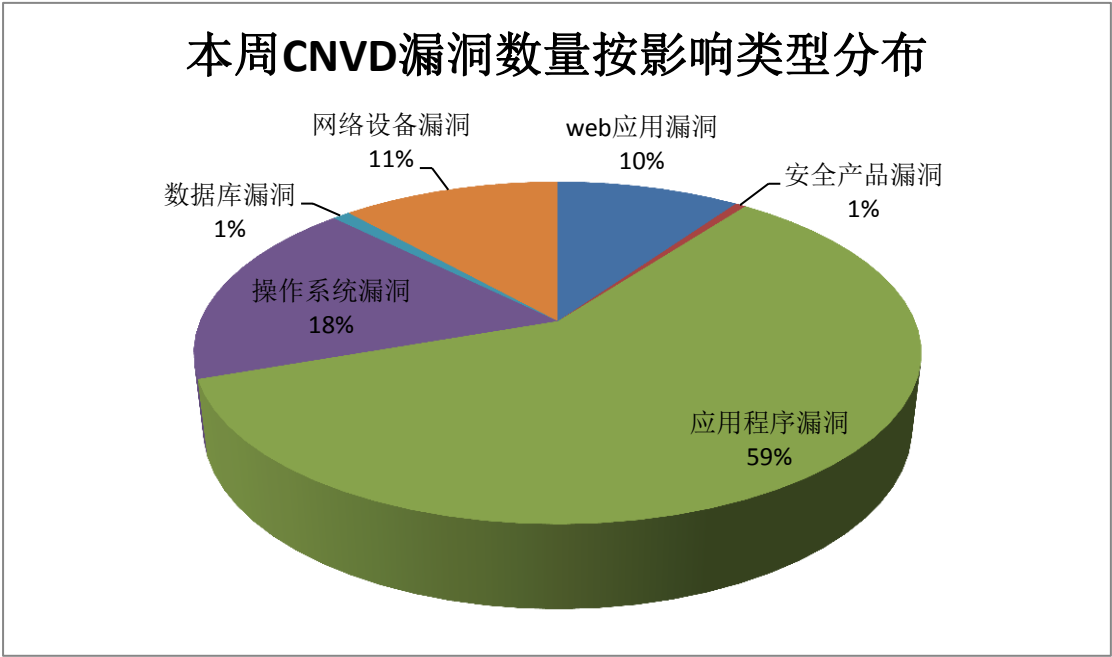


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、IBM、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	Linux	31	6%
2	IBM	31	6%
3	Microsoft	31	6%
4	HP	26	5%
5	Cisco	25	5%
6	Apple	23	4%
7	Circle Media	22	4%
8	Google	18	3%
9	IrfanView	16	3%
10	其他	311	58%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，71 个移动互联网行业漏洞(如下图所示)。其中，“Samsung GALAXY Apps 权限访问控制漏洞、多款 Huawei 产品输入验证漏洞、MitraStar GPT-2541GNAC (HGU)和 DSL-100HN-T1 权限提升漏洞、多款 Apple 产品 li

bc 拒绝服务漏洞、Google Android system (camera)权限提升漏洞”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/>

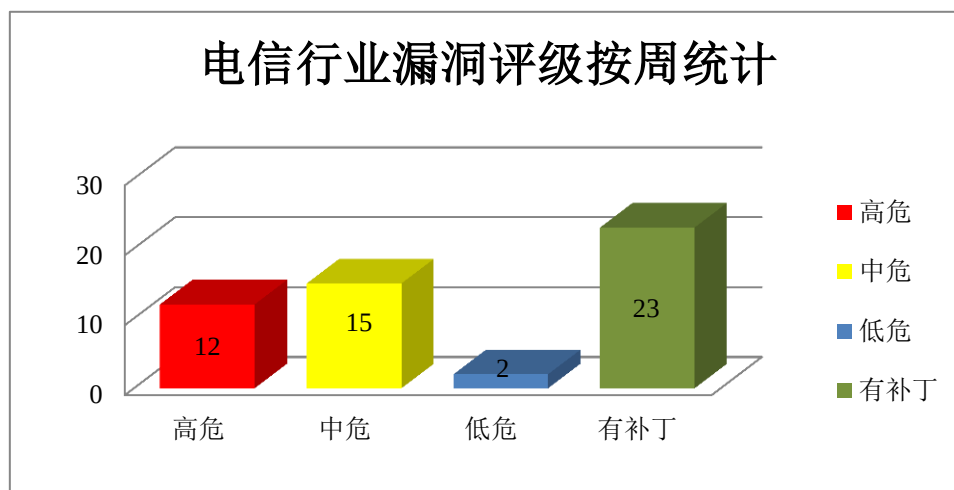


图 3 电信行业漏洞统计

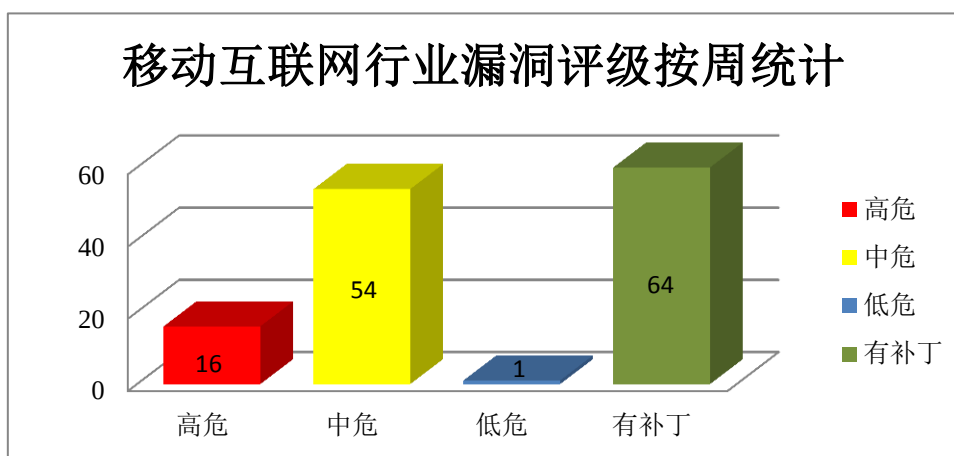


图 4 移动互联网行业漏洞统计

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、Apple 产品安全漏洞

Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。iCloud for Windows 是一款基于 Windows 平台的云服务。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在远程代码执行和内存破坏漏洞，

攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件远程代码执行漏洞（CNVD-2017-33557、CNVD-2017-33558、CNVD-2017-33559、CNVD-2017-33560、CNVD-2017-33561、CNVD-2017-33562）、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2017-32835、CNVD-2017-32836）。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-2017-33557>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33558>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33559>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33560>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33561>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33562>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32835>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32836>

2、Google 产品安全漏洞

Android 是美国谷歌公司的一套以 Linux 为基础的开源操作系统。Media framework 是其中的一个用于多媒体开发框架。Broadcom Wi-Fi driver 是其中的一个 Wi-Fi 驱动模块。本周，上述产品被披露存在权限提升和拒绝服务漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Android Broadcom wifi 权限提升漏洞、Google Android HTC bootloader 权限提升漏洞（CNVD-2017-32979）、Google Android Huawei bootloader 权限提升漏洞、Google Android Media Framework 拒绝服务漏洞（CNVD-2017-33337、CNVD-2017-33338、CNVD-2017-33339）、Google Android MediaTek soc driver 权限提升漏洞、Google Android Motorola bootloader 权限提升漏洞（CNVD-2017-32984）。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-2017-32986>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32979>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32982>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33337>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33338>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33339>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32983>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-32984>

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该产品被披露存在本地拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 本地拒绝服务漏洞(CNVD-2017-33091、CNVD-2017-33092、CNVD-2017-33093、CNVD-2017-33094、CNVD-2017-33095、CNVD-2017-33096、CNVD-2017-33097、CNVD-2017-33098)。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-2017-33091>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33092>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33093>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33094>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33095>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33096>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33097>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33098>

4、HP 产品安全漏洞

HP Intelligent Management Center (IMC) 是一个从底层构建的综合管理平台。本周，该产品被披露存在任意代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：HP Intelligent Management Center 任意代码执行漏洞 (CNVD-2017-33288、CNVD-2017-33289、CNVD-2017-33290、CNVD-2017-33529、CNVD-2017-33530、CNVD-2017-33531、CNVD-2017-33532、CNVD-2017-33533)。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-2017-33288>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33289>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33290>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33529>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33530>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33531>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33532>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33533>

5、Samsung NVR 设备密码泄露漏洞

Samsung NVR devices 是韩国三星 (Samsung) 公司的一款网络视频录像机设备。本周，Samsung 被披露存在密码泄露漏洞，远程攻击者可利用该漏洞读取管理员账户的 MD5 密码散列，并登录设备。目前，厂商尚未发布漏洞修补程序。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-2017-33219>

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>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-32885	GNU Wget 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://ftp.gnu.org/gnu/wget/
CNVD-2017-32886	GNU Wget 缓冲区错误漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://ftp.gnu.org/gnu/wget/
CNVD-2017-33058	SAP Point of Sale Xpress Server 身份验证绕过漏洞	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.sap.com
CNVD-2017-33059	SAP Point of Sale Xpress Server 访问认证漏洞	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.sap.com
CNVD-2017-33065	EMC AppSync 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.emc.com/
CNVD-2017-33191	QEMU 整数溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.qemu.org/
CNVD-2017-33192	OCaml compiler 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://ocaml.org/
CNVD-2017-33385	Cesanta Mongoose 拒绝服务漏洞	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://cesanta.com/
CNVD-2017-33388	Cesanta Mongoose MQTT 拒绝服务漏洞	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://cesanta.com/
CNVD-2017-33520	ZOHO ManageEngine Desktop Central 任意文件执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.manageengine.com

表 4 部分重要高危漏洞列表

小结：本周，Apple 被披露存在远程代码执行和内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Linux、HP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，Samsung 被披露存在密码泄露漏洞，远程攻击者可利用该漏洞读取管理员账户的 MD5 密码散列，并登录设备。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。



本周漏洞要闻速递

1. 多家反病毒软件存在 AVGater 问题，恶意软件反可利用隔离区提权

几款常见的反病毒软件中曝出存在一种可让攻击者利用隔离区来提升恶意软件权限的问题，涉及的反病毒软件厂商具体有趋势科技、Emisoft、卡巴斯基，Malwarebytes, Check Point (ZoneAlarm) 以及 Ikarus。攻击首先使用恶意 DLL 文件放入防病毒软件的隔离区。然后攻击者可以利用安全软件的 Windows 进程（SYSTEM 权限）来修复这个文件。一旦恶意 DLL 文件移动到了目标文件夹中，与该文件夹所关联的 Windows 进程自然就会执行相关的工作，恶意 DLL 就这样会被执行。

参考链接：<http://www.freebuf.com/news/153761.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