

信息安全漏洞周报

2017 年 07 月 03 日-2017 年 07 月 09 日

2017 年第 28 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 112 个、中危漏洞 162 个、低危漏洞 34 个。漏洞平均分为 6.05。本周收录的漏洞中，涉及 0day 漏洞 107 个（占 35%），其中互联网上出现“Avast Anti virus 本地权限提升漏洞”等零日代码攻击漏洞。此外，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 1011 个，与上周（1466 个）环比下降 31%。

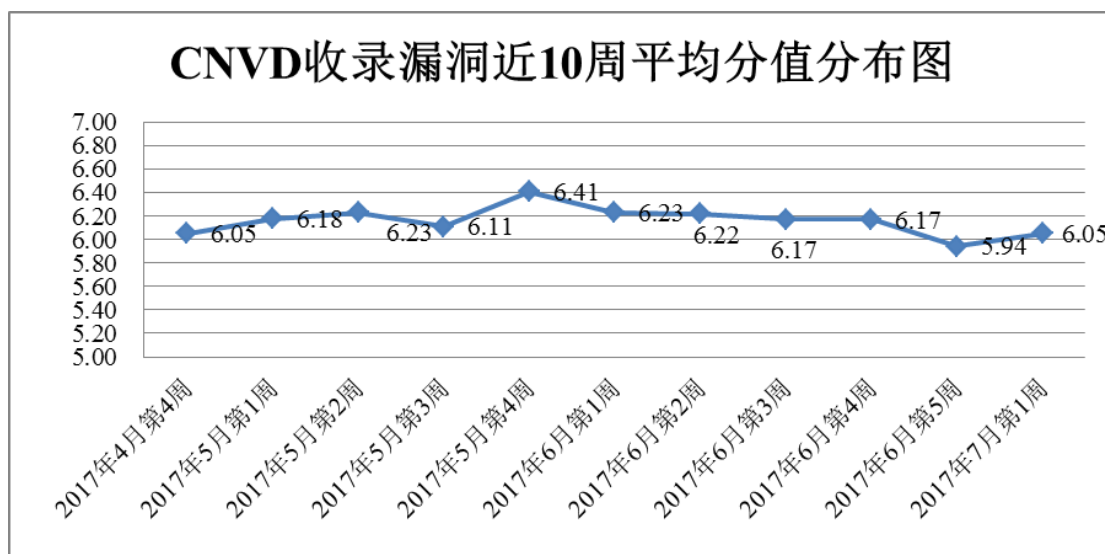


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、企业用户及个人用户报送了本周收录的全部 308 个漏洞。报送情况如表 1 所示。其中，华为技术有限公司、天融信、安天实验室、恒安嘉新、H3C 等单位报送数量较多。360 网神、漏洞盒子、南京联成科技发展股份有限公司、广州神月信息安全技术有限公司、六壬网安、中新网络信息安全股份有限公司、山石网科通

信技术有限公司、广州软云计算机科技有限公司、杭州朔方信息技术有限公司、北京安码科技有限公司、江苏君立华域信息安全技术有限公司、网信智安、长沙天融信网络安全技术有限公司、清远职业技术学院、安徽新华博信息技术股份有限公司、上海犇众信息技术有限公司及其他个人白帽子向 CNVD 提交了 1011 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
华为技术有限公司	244	0
天融信	223	2
漏洞盒子	143	143
安天实验室	120	0
恒安嘉新	115	0
H3C	115	0
启明星辰	88	5
中国电信集团系统集成有限责任公司	50	0
360 网神	48	48
绿盟科技	48	0
杭州安恒信息技术有限公司	41	0
厦门服云信息科技有限公司	25	0
广西鑫瀚科技有限公司	6	6
东软	5	5
北京数字观星科技有限公司	5	0
南京联成科技发展股份有限公司	37	37
广州神月信息安全技术有限公司	28	28
六壬网安	25	25
中新网络信息安全股	17	17

份有限公司		
山石网科通信技术有 限公司	13	13
广州软云计算科技 有限公司	11	11
杭州朔方信息技术有 限公司	10	10
北京安码科技有限公 司	4	4
江苏君立华域信息安 全技术有限公司	4	4
网信智安	4	4
长沙天融信网络安全 技术有限公司	2	2
清远职业技术学院	1	1
安徽新华博信息技术 股份有限公司	1	1
上海彝众信息技术有 限公司	1	1
山西分中心	9	9
吉林分中心	4	4
辽宁分中心	3	3
广东分中心	2	2
新疆分中心	2	2
浙江分中心	2	2
河北分中心	2	2
宁夏分中心	1	1
个人	619	619
报送总计	2065	1011
录入总计	308（去重）	1011

表 1 漏洞报送情况统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 308 个漏洞。其中应用程序漏洞 112 个，web 应用漏洞 99 个，操作系统漏洞 75 个，网络设备漏洞 17 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	112
web 应用漏洞	99
操作系统漏洞	75
网络设备漏洞	17
安全产品漏洞	5

表 2 漏洞按影响类型统计表

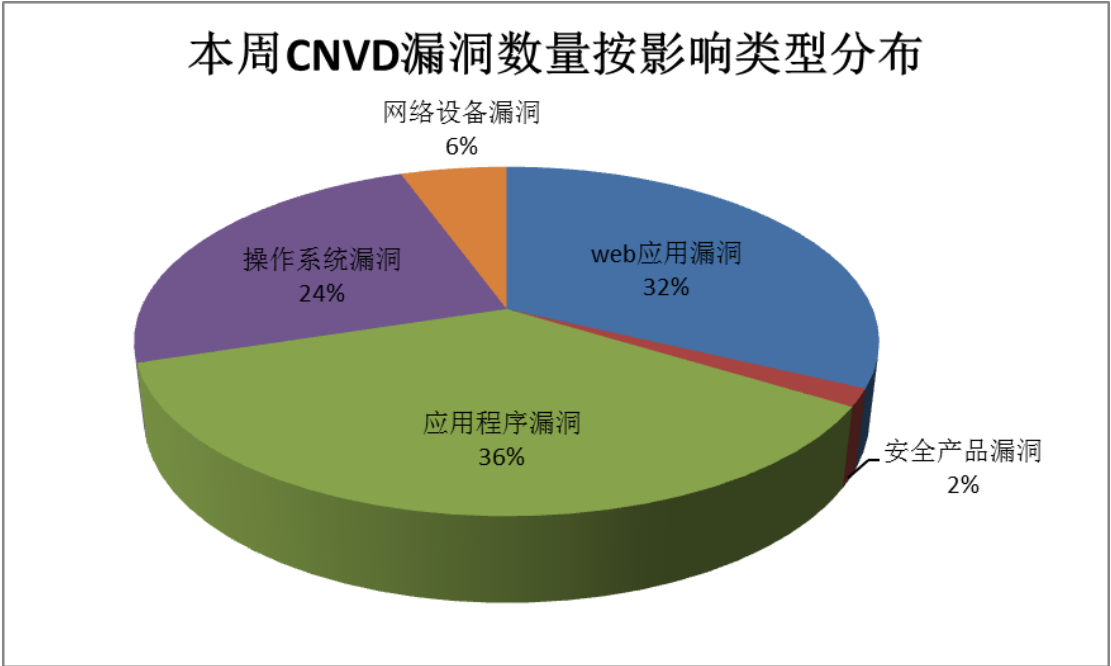


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft 、Mozilla、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。

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	52	17%
2	Mozilla	27	9%
3	Google	15	5%
4	Huawei	14	5%
5	Cisco	9	3%
6	LAME	7	2%
7	FFmpeg	7	2%

8	Wordpress	6	2%
9	IBM	6	2%
10	其他	165	53%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，19 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“Cisco IOS 和 IOS XE SNMP 远程执行代码漏洞、Aerohive HiveOS 存在多个漏洞、D-Link DIR-615 Wireless N 300 路由器验证绕过漏洞、Google Android WideVine DRM 安全绕过漏洞、Google Android Qualcomm Sound 驱动程序权限提升漏洞、Google Android Qualcomm Video 驱动程序权限提升漏洞、Google Android 存在未明漏洞（CNVD-2017-13248、CNVD-2017-13249）”等的综合评级为“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/>

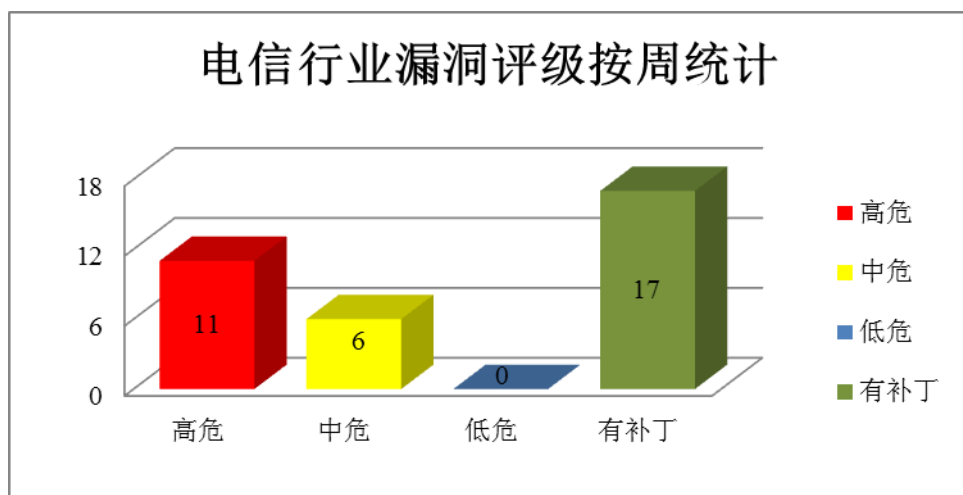


图 3 电信行业漏洞统计

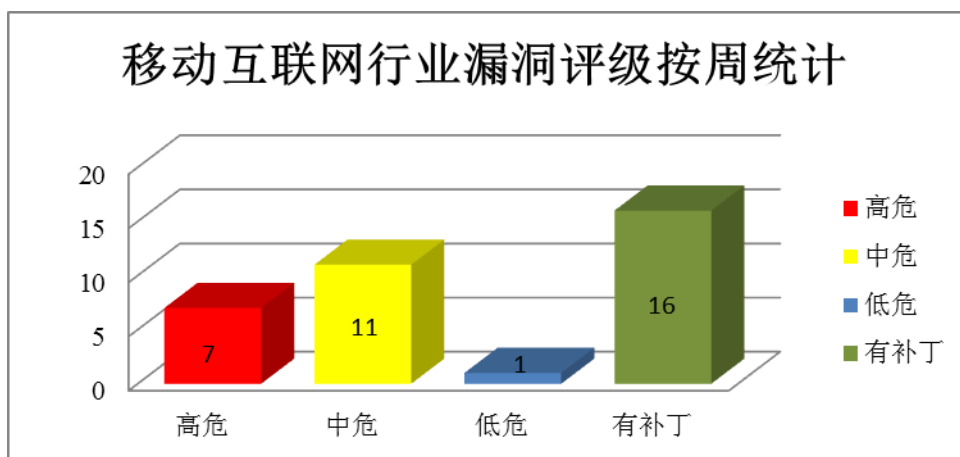


图 4 移动互联网行业漏洞统计

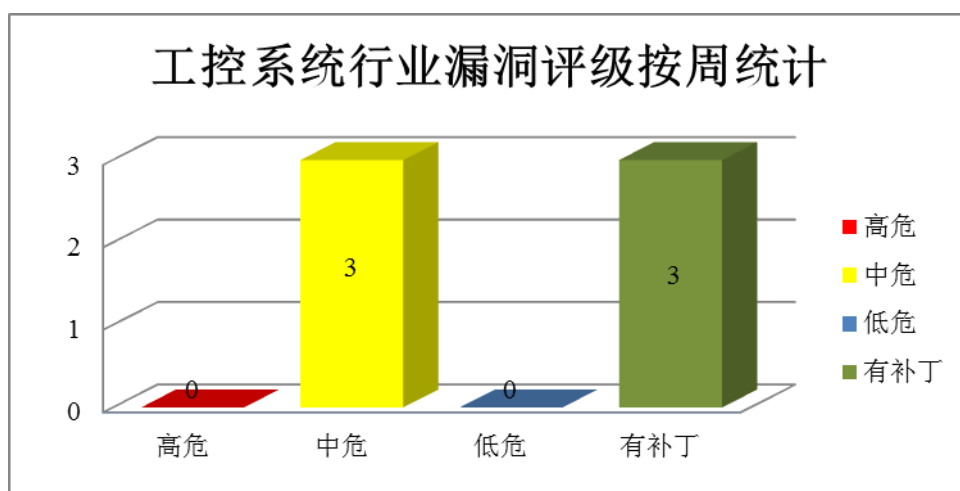


图 5 工控系统行业漏洞统计

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、Apache Struts(S2-048)远程命令执行漏洞

Apache Struts 是一款用于创建企业级 Java Web 应用的开源框架。本周，该产品被披露存在远程命令执行漏洞，攻击者可通过构建不可信的输入实现远程命令攻击。

CNVD 收录的相关漏洞包括：Apache Struts(S2-048)远程命令执行漏洞。该漏洞的综合评级为“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-2017-13259>

2、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。本周，该产品被披露存在本地权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限和执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows 本地权限提升漏洞（CNVD-2017-13004、CNVD-2017-13005、CNVD-2017-13006、CNVD-2017-12997）、Microsoft Windows 远程代码执行漏洞（CNVD-2017-12778、CNVD-2017-12779、CNVD-2017-12780、CNVD-2017-12782）。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-2017-13004>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-13005>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-13006>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12997>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12778>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12779>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12780>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12782>

3、Huawei 产品安全漏洞

Huawei Unified Maintenance Audit (UMA)是为运营商、政府、金融、电力、大企业等设计的统一 IT 核心资源运维管理与安全审计平台。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Huawei UMA 产品权限提升漏洞（CNVD-2017-12925、CNVD-2017-12926、CNVD-2017-12927、CNVD-2017-12928、CNVD-2017-12929、CNVD-2017-12930、CNVD-2017-12931、CNVD-2017-12932）。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-2017-12925>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12926>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12927>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12928>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12929>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12930>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12931>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12932>

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互连网络操作系统。本周，该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：Cisco IOS 和 IOS XE SNMP 远程执行代码漏洞（CNVD-2017-12528、CNVD-2017-12529、CNVD-2017-12530、CNVD-2017-12531、CNV

D-2017-12532、CNVD-2017-12533、CNVD-2017-12534、CNVD-2017-12535)。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-2017-12528>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12529>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12530>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12531>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12532>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12533>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12534>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12535>

5、HP PageWide Printers/HP OfficeJet Pro Printers 任意代码执行漏洞

HP Officejet 8500A 是惠普出品的打印/复印/扫描/传真多功能一体机。本周，HP 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。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2017-13140>

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-2017-12537	ISC BIND 安全绕过漏洞 (CNVD-2017-12537)	中	用户可联系供应商获得补丁信息： http://www.isc.org/downloads
CNVD-2017-12591	AMAX Winmail Server 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/zhonghaozhao/winmail/issues/1
CNVD-2017-12975	Sitecore CMS 'searchStr'参数跨站脚本漏洞	中	厂商已发布漏洞修复程序，请及时关注更新： http://seclists.org/bugtraq/2017/Jun/43
CNVD-2017-12974	LAME lame_init_params 函数拒绝服务漏洞	中	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://sourceforge.net/projects/lame/
CNVD-2017-12973	LAME fill_buffer_resample 函数拒绝服务漏洞	中	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://sourceforge.net/projects/lame/
CNVD-201	lrzip 'get_fileinfo'函数栈溢出漏洞	中	用户可参考如下厂商提供的安全补

7-12968	洞		丁以修复该漏洞： http://lrzip.kolivas.org
CNVD-2017-12967	lrzip 'get_fileinfo'函数栈溢出漏洞	中	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://lrzip.kolivas.org
CNVD-2017-12964	Silicon Graphics LibTIFF 堆缓冲区溢出漏洞	中	用户可联系供应商获得补丁信息： http://www.libtiff.org/
CNVD-2017-12992	Mosquitto 信息泄露漏洞	低	厂商已发布漏洞修复程序，请及时关注更新： https://mosquitto.org/files/cve/2017-9868/
CNVD-2017-13257	Elasticsearch Kibana 开放重定向漏洞	中	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www.elastic.co/community/security

表 4 部分重要高危漏洞列表

小结：本周，Apache 被披露存在远程命令执行漏洞，攻击者可通过构建不可信的输入实现远程命令攻击。此外，Microsoft、Huwei、Cisco 等多款产品被披露存在多个漏洞，攻击者利用漏洞可提升权限或执行任意命令。另外，HP 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。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. Struts2 showcase 远程代码执行漏洞（S2-048）

来自斗象科技（Tophant）的安全研究员 icez 发现 Struts2 showcase 应用中存在远程代码执行高危漏洞。Struts2 官方已经确认该漏洞（漏洞编号 S2-048，CVE 编号：CVE-2017-9791），在 Struts 2.3.x 系列的 Showcase 应用中演示 Struts2 整合 Struts 1 的插件中存在一处任意代码执行漏洞。当你的应用使用了 Struts2 Struts1 的插件时，可能导致不受信任的输入传入到 ActionMessage 类中导致命令执行。

参考链接：<http://www.freebuf.com/news/139644.html>

2. Skype 曝出远程栈缓冲区溢出漏洞

来自德国安全公司 Vulnerability Lab 的安全研究专家 Benjamin Kunz-Mejri 在目前国外最热门的免费 Web 信息与语音呼叫服务 Skype 中发现了一个严重的安全漏洞（CVE-2017-9948）。据了解，这个 0 day 漏洞属于远程栈缓冲区溢出漏洞，而这个漏洞或将允许任意攻击者远程执行恶意代码并导致系统发生崩溃。Skype 是一款免费的在线服务，它允许用户通过文字、语音和视频等方式与自己的好友进行即时通信。

参考链接：<http://www.freebuf.com/news/138822.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：010-82990999