

信息安全漏洞周报

2017 年 08 月 14 日-2017 年 08 月 20 日

2017 年第 34 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**高**。

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 397 个，其中高危漏洞 160 个、中危漏洞 220 个、低危漏洞 17 个。漏洞平均分为 6.68。本周收录的漏洞中，涉及 0day 漏洞 90 个（占 23%），其中互联网上出现“Joomla SocialPinBoard 插件任意文件上传漏洞、Humax Digital HG100R 备份文件下载漏洞”等零日代码攻击漏洞。本周，Xshell 后门险的披露使得针对服务器主机的安全威胁较高。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 1493 个，与上周（1665 个）环比下降 10%

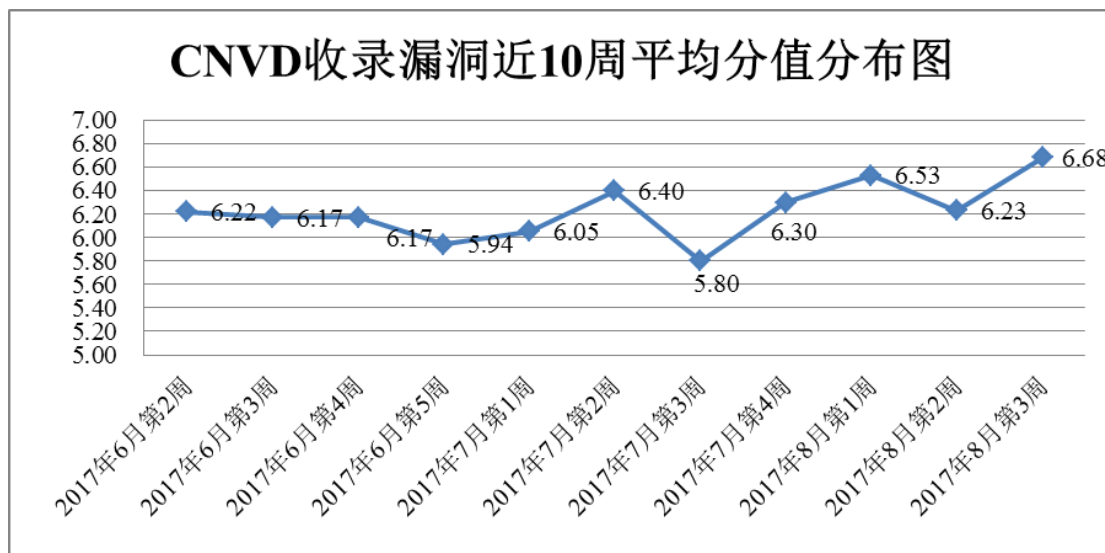


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 家成员单位、企业用户及个人用户报送了本周收录的全部 397 个漏洞。报送情况如表 1 所示。其中，华为技术有限公司、安天实验室、H3C、天融信、东软等

单位报送数量较多。山石网科通信技术有限公司、中新网络信息安全股份有限公司、北京安码科技有限公司、深圳市鼎安天下信息科技有限公司、上海彝众信息技术有限公司、安徽新华博信息技术股份有限公司、江西安服信息产业有限公司、六壬网安、智容科技有限公司、中国航天科工集团第四研究院软件评测中心（北京）、广州神月信息安全技术有限公司、江苏同袍信息科技有限公司、南京联成科技发展股份有限公司及其他个人白帽子向 CNVD 提交了 1493 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
漏洞盒子	428	428
华为技术有限公司	387	0
360 网神	232	232
安天实验室	195	0
H3C	189	0
天融信	144	1
东软	134	3
中国电信集团系统集成有 限责任公司	130	29
启明星辰	93	9
厦门服云信息科技有限公 司	65	1
恒安嘉新	63	0
绿盟科技	54	0
北京数字观星科技有限公 司	49	0
杭州安恒信息技术有限公 司	45	0
知道创宇	1	1
北京无声信息技术有限公 司	1	0
山石网科通信技术有限公 司	48	48
中新网络信息安全股份有 限公司	18	18

北京安码科技有限公司	11	11
深圳市鼎安天下信息科技有限公司	8	8
上海犇众信息技术有限公司	4	4
安徽新华博信息技术股份有限公司	3	3
江西安服信息产业有限公司	3	3
六壬网安	2	2
智容科技有限公司	2	2
中国航天科工集团第四研究院软件评测中心（北京）	2	2
广州神月信息安全技术有限公司	1	1
江苏同袍信息科技有限公司	1	1
南京联成科技发展股份有限公司	1	1
CNCERT 吉林分中心	4	4
CNCERT 宁夏分中心	4	4
CNCERT 广东分中心	2	2
CNCERT 陕西分中心	2	2
CNCERT 河北分中心	1	1
个人	672	672
报送总计	2999	1493
录入总计	397（去重）	1493

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 397 个漏洞。其中应用程序漏洞 287 个，web 应用漏洞 68 个，操作系统漏洞 19 个，网络设备漏洞 17 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	287
web 应用漏洞	68
操作系统漏洞	19
网络设备漏洞	17
安全产品漏洞	6

表 2 漏洞按影响类型统计表

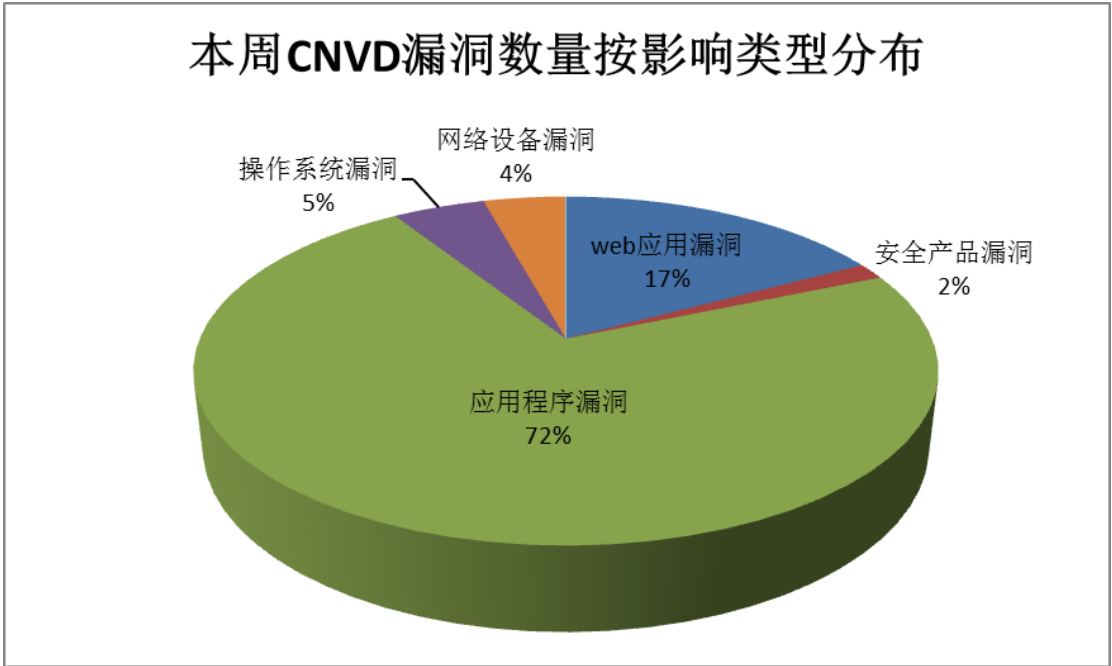


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 HP、IBM、ImageMagick 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	HP	60	15%
2	IBM	44	11%
3	ImageMagick	39	10%
4	Oracle	19	5%
5	GNU	13	3%
6	Google	9	2%
7	Adobe	8	2%
8	Juniper Networks	7	2%
9	Liferay	6	2%
10	其他	192	48%

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 10 个电信行业漏洞，33 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Google Android framework 权限提升漏洞（CNVD-2017-21536、CNVD-2017-21537、CNVD-2017-21538）、Google Android System UI 远程代码执行漏洞（CNVD-2017-21550、CNVD-2017-21551）”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/>

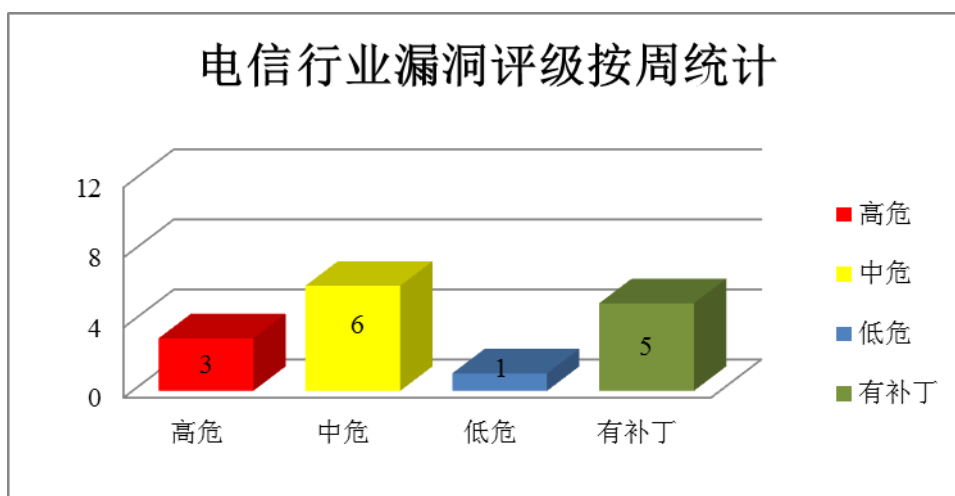


图 3 电信行业漏洞统计

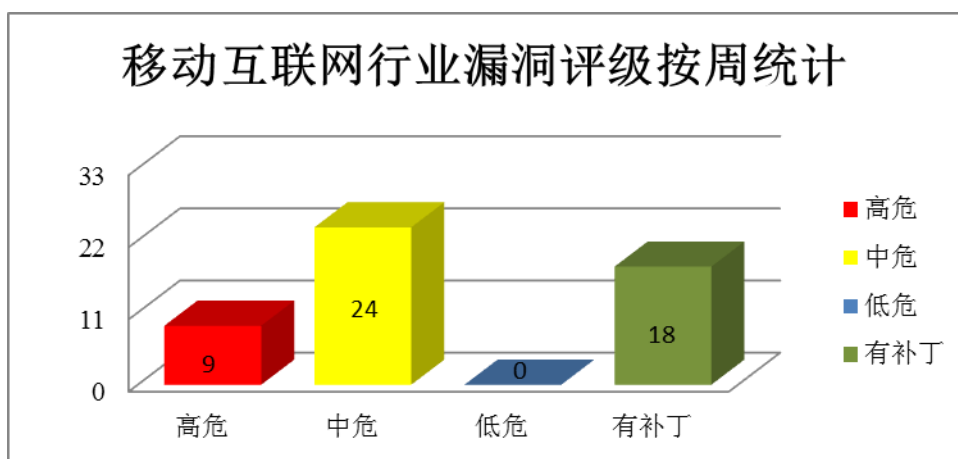


图 4 移动互联网行业漏洞统计

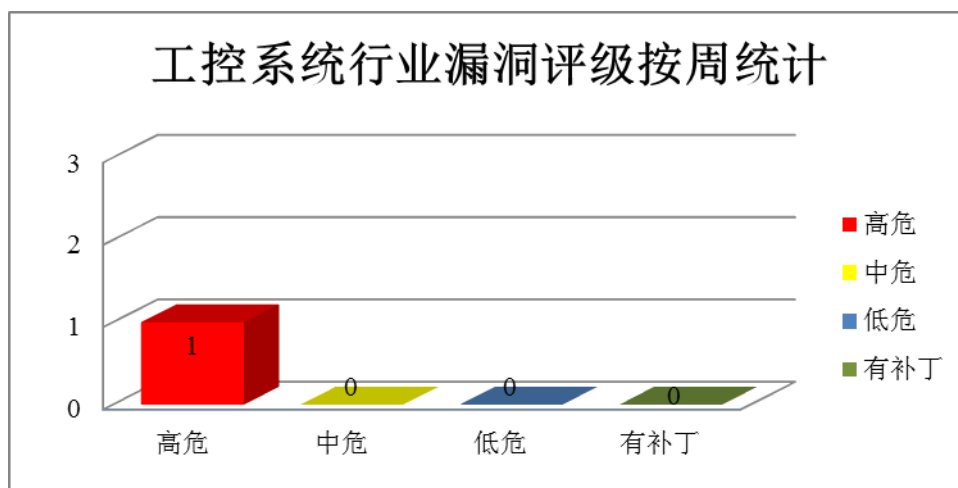


图 5 工控系统行业漏洞统计

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、NetSarang Xmanager 和 Xshell 等多款产品安全漏洞

NetSarang 是一家提供安全链接解决方案的公司，Xshell 是一款终端模拟软件。本周，该产品被披露存在后门漏洞，攻击者可利用漏洞泄露敏感信息。

CNVD 收录的相关漏洞包括：NetSarang Xmanager 和 Xshell 等多款产品 nssock2.dll 模块存在后门。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-2017-21513>

2、HP 产品安全漏洞

HPE Intelligent Management Center (iMC) PLAT 是美国惠普企业（Hewlett Packard Enterprise, HPE）公司的一套网络智能管理中心解决方案。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：HPE Intelligent Management Center PLAT 任意代码执行漏洞（CNVD-2017-21562、CNVD-2017-21563、CNVD-2017-21564、CNVD-2017-21565、CNVD-2017-21566、CNVD-2017-21567、CNVD-2017-21568、CNVD-2017-21569）。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-2017-21562>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21564>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21565>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21566>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21567>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21568>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21569>

3、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款流行的处理 PDF 文件的应用程序。Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。本周，上述产品被披露存在内存破坏和信息泄露漏洞，攻击者可利用漏洞执行任意的代码或泄露敏感信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2017-21193、CNVD-2017-21194、CNVD-2017-21195、CNVD-2017-21196、CNVD-2017-21197、CNVD-2017-21198、CNVD-2017-21199）、Adobe Flash Player 信息泄露漏洞（CNVD-2017-21200）。除“Adobe Flash Player 信息泄露漏洞（CNVD-2017-21200）”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-2017-21193>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21194>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21195>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21196>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21197>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21198>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21199>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21200>

4、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，该产品被披露存在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或执行任意代码。

CNVD 收录的相关漏洞包括：Google Android framework 权限提升漏洞、Google Android framework 权限提升漏洞（CNVD-2017-21536、CNVD-2017-21537、CNVD-2017-21538）、Google Android System UI 远程代码执行漏洞（CNVD-2017-21549、CNVD-2017-21550、CNVD-2017-21551、CNVD-2017-21552）。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-2017-21539>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21536>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21537>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21538>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21549>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-21552>

5、Schneider Electric Pro-Face WinGP 任意代码执行漏洞

Pro-Face GP Pro-Server EX 是支持专用和开放 HMI（基于 PC）解决方案的首选 HMI 开发软件。本周，Schneider Electric 被披露存在任意代码执行漏洞，攻击者可利用漏洞在进程的上下文中执行任意代码。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-2017-21360>

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-2017-21032	Trend Micro OfficeScan 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://success.trendmicro.com/solution/1117769
CNVD-2017-21507	Perl DBD::mysql 模块拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://github.com/perl5-dbi/DBD-mysql/issues/120
CNVD-2017-21510	VideoLAN VLC avcodec 拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://trac.videolan.org/vlc/ticket/18467
CNVD-2017-21546	MCollective 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://puppet.com/security/cve/cve-2017-2292
CNVD-2017-21728	Xen 权限提升漏洞（CNVD-2017-21728）	高	厂商已发布漏洞修复程序，请及时关注更新： https://xenbits.xen.org/xsa/advisory-22.html
CNVD-2017-21732	Xen 存在多个漏洞（CNVD-2017-21732）	高	厂商已发布漏洞修复程序，请及时关注更新： https://xenbits.xen.org/xsa/advisory-218.html
CNVD-2017-21734	Odoo 认证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://github.com/odoo/odoo/issues/1

			7914
CNVD-2017-21742	Fortinet FortiWLM 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://fortiguard.com/advisory/FG-IR-17-115
CNVD-2017-21747	Xen grant-table 功能拒绝服务漏洞（CNVD-2017-21747）	高	厂商已发布漏洞修复程序，请及时关注更新： https://xenbits.xen.org/xsa/advisory-224.html
CNVD-2017-21748	Xen grant-table 功能拒绝服务漏洞（CNVD-2017-21748）	高	厂商已发布漏洞修复程序，请及时关注更新： https://xenbits.xen.org/xsa/advisory-224.html

表 4 部分重要高危漏洞列表

小结：本周，NetSarang 被披露存在后门漏洞，攻击者可利用漏洞泄露敏感信息。此外，HP、Google、Adobe 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、执行任意代码或泄露敏感信息等。另外，Schneider Electric 被披露存在任意代码执行漏洞，攻击者可利用漏洞在进程的上下文中执行任意代码。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. Xshell 系列软件被植入后门

Xshell 是一个强大的安全终端模拟软件，它支持 SSH1, SSH2, 以及 Microsoft Windows 平台的 TELNET 协议。Xshell 通过互联网到远程主机的安全连接以及它创新性的设计和特色帮助用户在复杂的网络环境中享受他们的工作。用户可通过查看 nssock2.dll 的版本来确定是否受此影响：在软件安装目录下找到 nssock2.dll 文件，右键该文件查看属性，如果版本号为 5.0.0.26 则存在后门代码。

参考链接：<http://www.freebuf.com/news/144124.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