

信息安全漏洞周报

2017 年 11 月 20 日-2017 年 11 月 26 日

2017 年第 48 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 277 个，其中高危漏洞 71 个、中危漏洞 195 个、低危漏洞 11 个。漏洞平均分为 5.95。本周收录的漏洞中，涉及 0day 漏洞 49 个（占 18%），其中互联网上出现“SimpleXML XML 外部实体注入漏洞、Berta CMS 任意文件上传漏洞”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 509 个，与上周（772 个）环比减少 34%。

CNVD收录漏洞近10周平均分分布图

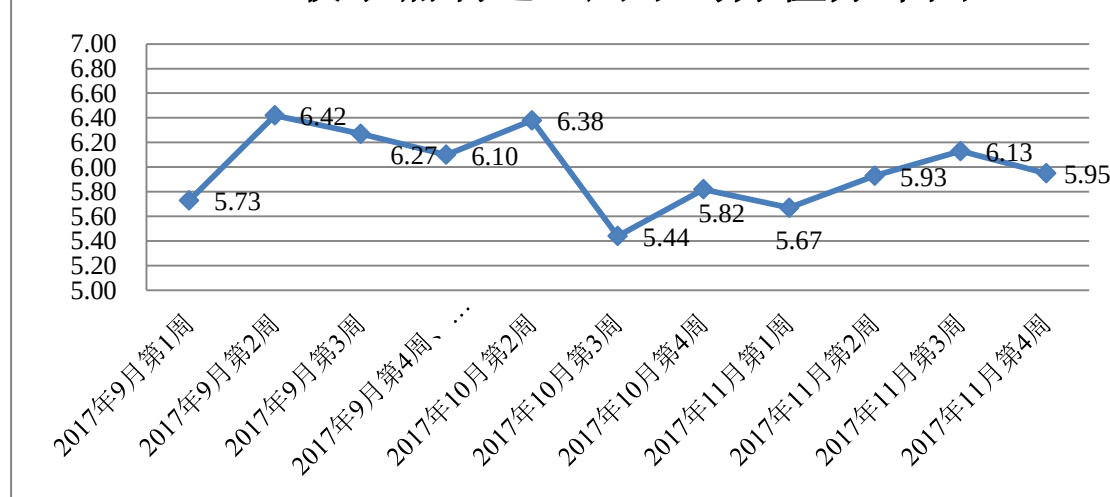


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天融信、H3C、绿盟科技、启明星辰、安天实验室等单位报送数量较多。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、深圳市鼎安天下信息科技有限公司、聚锋信息安全实验室、漏斗社区、

福建省海峡信息技术有限公司、广州软云计算机科技有限公司、广州万方计算机科技有限公司及其他个人白帽子向 CNVD 提交了 509 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
天融信	311	12
H3C	206	0
绿盟科技	155	16
启明星辰	117	0
网神	114	114
安天实验室	107	0
华为技术有限公司	101	0
恒安嘉新	101	0
中国电信集团系统集成有 限责任公司	53	0
杭州安恒信息技术有限公 司	49	0
漏洞盒子	38	38
东软	1	1
知道创宇	1	0
四川虹微技术有限公司 (子午攻防实验室)	20	20
中新网络信息安全股份有 限公司	19	19
深圳市鼎安天下信息科技 有限公司	9	9
聚锋信息安全实验室	1	1
漏斗社区	1	1
福建省海峡信息技术有限 公司	1	1
广州软云计算机科技有限 公司	1	1

广州万方计算机科技有限公司	1	1
CNCERT 新疆分中心	14	14
CNCERT 江西分中心	8	8
CNCERT 福建分中心	5	5
CNCERT 海南分中心	4	4
CNCERT 广东分中心	2	2
个人	242	242
报送总计	1682	509



本周漏洞按类型和厂商统计

本周，CNVD 收录了 277 个漏洞。其中应用程序漏洞 169 个，操作系统漏洞 46 个，web 应用漏洞 34 个，网络设备漏洞 16 个，安全产品漏洞 10 个，数据库漏洞 2 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	169
操作系统漏洞	46
web 应用漏洞	34
网络设备漏洞	16
安全产品漏洞	10
数据库漏洞	2

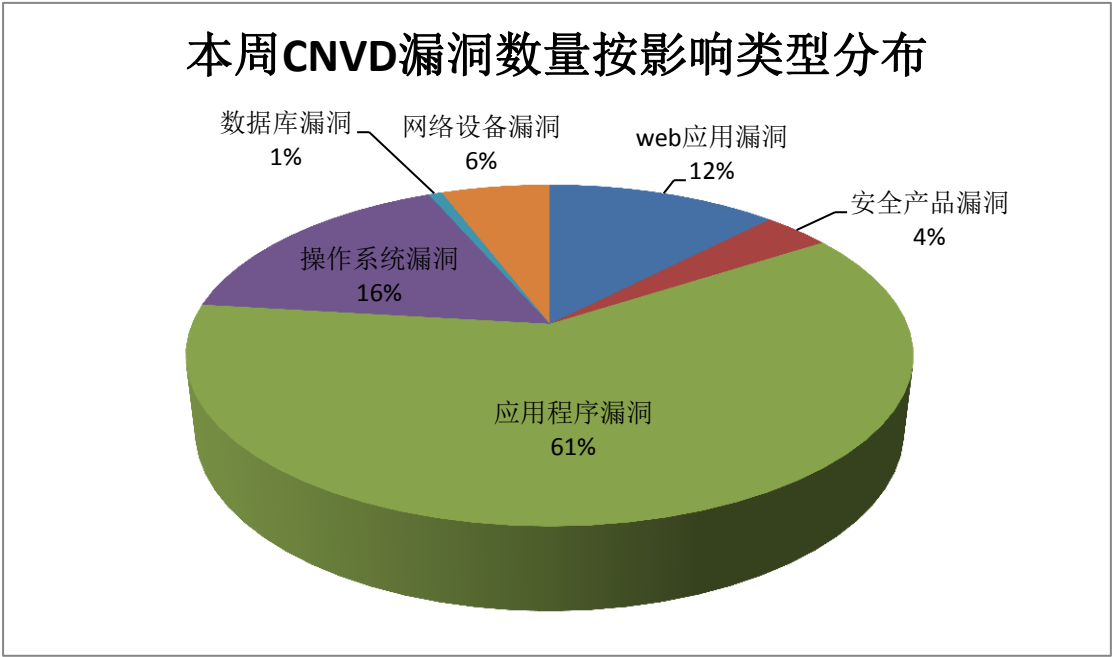


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Cisco、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	Google	43	16%
2	Cisco	23	8%
3	Microsoft	19	7%
4	WordPress	10	4%
5	GNU	8	3%
6	libeblm2	7	3%
7	IBM	6	2%
8	Huawei	6	2%
9	Red Hat	5	2%
10	其他	150	53%

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，44 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 Umbrella Insights Virtual Appliances 本地权限提升漏洞、Intel Unite App admin portal 权限提升漏洞、Google Android Qualcomm Camer

a 提权漏洞、Android Kernel Audio 驱动程序权限提升漏洞、Android System inputdispatcher 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/>

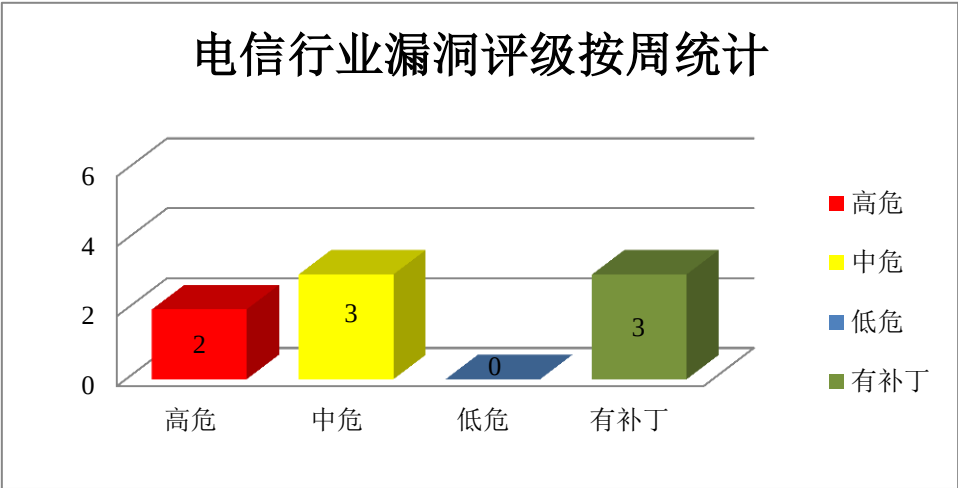


图 3 电信行业漏洞统计

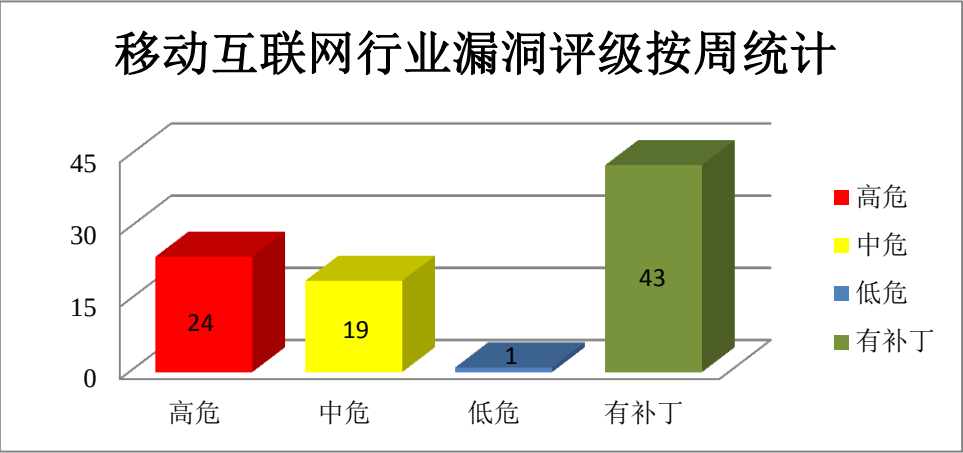


图 4 移动互联网行业漏洞统计

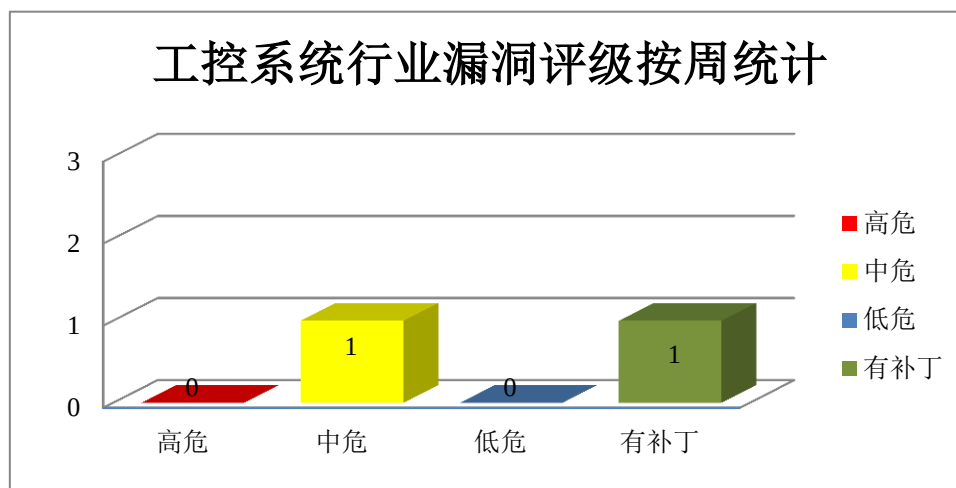


图 5 工控行业漏洞统计

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、Red Hat JBoss Enterprise Application Platform 远程代码执行漏洞

Red Hat JBoss Enterprise Application Platform (EAP) 是美国红帽 (Red Hat) 公司的一套开源、基于 J2EE 的中间件平台。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：Red Hat JBoss Enterprise Application Platform 远程代码执行漏洞 (CNVD-2017-33724)。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-2017-33724>

2、Google 产品安全漏洞

Android on Google Pixel 和 Nexus 是美国谷歌的一套运行于 Google Pixel 和 Nexus 中并以 Linux 为基础的开源操作系统。Qualcomm Camera 是使用在其中的一个摄像头程序。本周，上述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：Android Qualcomm Audio 权限提升漏洞、Android Qualcomm Camera 权限提升漏洞、Android Qualcomm Camera 权限提升漏洞 (CNVD-2017-34667、CNVD-2017-34673)、Android Qualcomm Linux kernel 权限提升漏洞、Android Qualcomm Memory 子系统权限提升漏洞、Android Qualcomm Services 权限提升漏洞、Android Qualcomm WLAN 权限提升漏洞。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-2017-34670>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34666>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34667>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34673>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34674>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34675>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34668>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34646>

3、Microsoft 产品安全漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge 脚本引擎内存破坏漏洞（CNVD-2017-34922、CNVD-2017-34923、CNVD-2017-34924、CNVD-2017-34927、CNVD-2017-34928、CNVD-2017-34932）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2017-34718、CNVD-2017-34719）。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-2017-34922>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34923>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34924>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34927>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34928>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34932>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34718>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34719>

4、Cisco 产品安全漏洞

Cisco Registered Envelope Service 是美国思科公司的一套邮件服务解决方案。Cisco Umbrella Insights Virtual Appliances 是一款基于云的安全互联网网关设备。Cisco IP Phone 8800 是一款提供视频和 VoIP 通信功能的电话产品。Cisco NX-OS 软件是一个数据中心级的操作系统。本周，上述产品被披露存在权限提升、命令注入和跨站脚本漏洞，攻击者可利用漏洞提升权限、执行任意命令或发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Cisco IP Phone 8800 系列 debug 界面命令注入漏洞、Cisco NX-OS Python 脚本引擎权限提升漏洞、Cisco Registered Envelope Service 跨站脚本漏洞（CNVD-2017-34809、CNVD-2017-34810、CNVD-2017-34811、CNVD-2017-34812、CNVD-2017-34813）、Cisco Umbrella Insights Virtual Appliances 本地权限提升

漏洞。其中，“Cisco IP Phone 8800 系列 debug 界面命令注入漏洞、Cisco NX-OS Python 脚本引擎权限提升漏洞、Cisco Umbrella Insights Virtual Appliances 本地权限提升漏洞”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-2017-34931>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34579>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34809>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34810>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34811>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34812>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34813>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34919>

5、Icinga Core 权限提升漏洞

Icinga Core 是 Icinga 项目的一套企业级开源监控系统。本周，Icinga 被披露存在权限提升漏洞，本地攻击者可利用该漏洞获取权限。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-2017-34963>

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-2017-34510	TerraMaster TOS shell 元字符注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://gist.github.com/hybriz/63bbe2d963e531357aca353c74dd1ad5
CNVD-2017-34695	Git 操作系统命令注入漏洞	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： https://git-scm.com/
CNVD-2017-34706	Ruby 安全绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://www.ruby-lang.org/en/news/2017/09/14/ruby-2-3-5-released/
CNVD-2017-34799	EMC Elastic Cloud Storage 默认密码漏洞	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-2017-34848	rbenv 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/rbenv/rbenv/issues/977

CNVD-2017-34850	多款 Thales nShield Connect 硬件权限访问控制漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.thales-esecurity.com/
CNVD-2017-34905	PNP4Nagios 权限提升漏洞	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/linge/pnp4nagios/issues/140
CNVD-2017-34957	QuickerBB 任意文件写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/halojoy/QuickerBB/issues/10
CNVD-2017-34958	ROOT xrootd 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://github.com/xrootd/xrootd/blob/v4.6.1/docs/ReleaseNotes.txt
CNVD-2017-34975	Gentoo app-admin/logstash-bin 软件包权限获取漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://bugs.gentoo.org/show_bug.cgi?id=628558

表 4 部分重要高危漏洞列表

小结：本周，Red Hat 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。此外，Google、Microsoft、Cisco 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跨站脚本攻击等。另外，Icinga 被披露存在权限提升漏洞，本地攻击者可利用该漏洞获取权限。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. 惠普企业打印机被曝含多种安全漏洞

近期，研究人员在某些型号的惠普企业打印机中发现了多个严重的安全漏洞（包括远程代码执行漏洞），全研究人员首先使用 PRET（打印机漏洞利用工具包）对设备进行了测试，并成功找到了一个路径遍历漏洞，而这个漏洞允许他们访问任意打印机任务的内容，其中也包括受密码保护的打印机任务。除此之外，PRET 还帮助他们找到了一个能够修改打印机任务内容的漏洞，一个能够将打印机恢复出厂设置的漏洞，还有一个能够移除管理员密码的漏洞。厂商表示已经在着手开发相应的漏洞补丁，客户在本周即可获得到相应的更新补丁。

参考链接：<http://www.freebuf.com/news/154965.html>

2. 兄弟牌网络打印机被曝存在远程 DoS 漏洞

近期，Trustwave 实验室发现兄弟牌（Brother）网络打印机的 Debut 嵌入式 web 服务前端存在漏洞，攻击者只需向目标打印机发送一个简单的 HTTP POST 畸形请求，就可对目标打印机形成远程 DoS 攻击。截至目前，全球有 14000 多台暴露在互联网的 Brother 打印机可能会受到该漏洞影响。

参考链接：<http://www.freebuf.com/news/154684.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