

信息安全漏洞周报

2017 年 08 月 21 日-2017 年 08 月 27 日

2017年第35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 292 个，其中高危漏洞 98 个、中危漏洞 180 个、低危漏洞 14 个。漏洞平均分为 6.21。本周收录的漏洞中，涉及 0day 漏洞 60 个（占 21%），其中互联网上出现“Joomla! Calendar Planner 组件 SQL 注入漏洞、NexusPHP SQL 注入漏洞”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 1483 个，与上周（1493 个）基本持平。

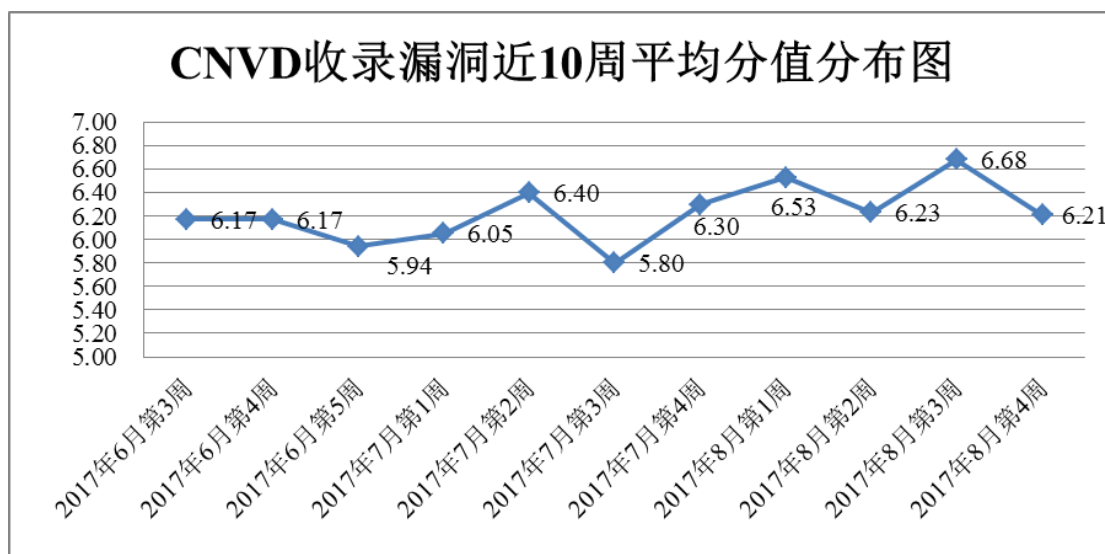


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 18 家成员单位、企业用户及个人用户报送了本周收录的全部 292 个漏洞。报送情况如表 1 所示。其中，H3C、天融信、安天实验室、华为技术有限公司、启明星辰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、

江苏同袍信息科技有限公司、华讯方舟通信设备有限公司、深圳市鼎安天下信息科技有限公司、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、北京安码科技有限公司、杭州朔方信息技术有限公司、江西卓安网络科技有限公司、湖南省金盾信息安全等级保护评估中心有限公司、北京市电子产品质量检测中心、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 1483 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
360 网神	241	241
H3C	196	0
天融信	186	0
漏洞盒子	179	179
安天实验室	159	0
华为技术有限公司	135	0
启明星辰	130	4
恒安嘉新	115	0
中国电信集团系统集成有 限责任公司	112	26
杭州安恒信息技术有限公 司	57	0
北京数字观星科技有限公 司	43	0
绿盟科技	42	0
厦门服云信息科技有限公司	14	0
深圳市深信服电子科技有 限公司	6	6
东软	7	7
北京无声信息技术有限公 司	2	0
广西鑫瀚科技有限公司	2	2
南京铨迅信息技术股份有 限公司	1	1
山石网科通信技术有限公	34	34

司		
中新网络信息安全股份有限公司	12	12
江苏同袍信息科技有限公司	9	9
华讯方舟通信设备有限公司	8	8
深圳市鼎安天下信息科技有限公司	8	8
安徽新华博信息技术股份有限公司	7	7
上海彝众信息技术有限公司	5	5
北京安码科技有限公司	4	4
杭州朔方信息技术有限公司	4	4
江西卓安网络科技有限公司	4	4
湖南省金盾信息安全等级保护评估中心有限公司	2	2
北京市电子产品质量检测中心	1	1
广州万方计算机科技有限公司	1	1
CNCERT 宁夏分中心	4	4
CNCERT 广东分中心	4	4
个人	910	910
报送总计	2644	1483
录入总计	292（去重）	1483

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 292 个漏洞。其中应用程序漏洞 199 个，web 应用漏洞 38 个，网络设备漏洞 26 个，操作系统漏洞 22 个，数据库漏洞 4 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
----------	------

应用程序漏洞	199
web 应用漏洞	38
网络设备漏洞	26
操作系统漏洞	22
数据库漏洞	4
安全产品漏洞	3

表 2 漏洞按影响类型统计表

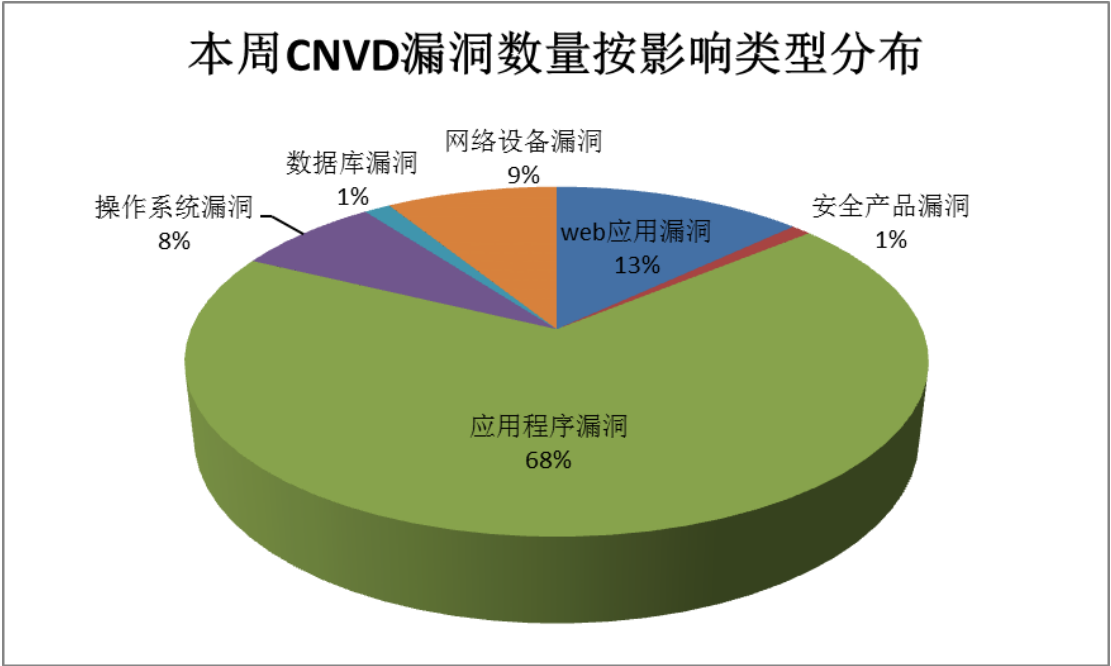


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、Adobe、Cisco 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	Mozilla	26	9%
2	Adobe	26	9%
3	Cisco	24	8%
4	Microsoft	16	5%
5	Google	15	5%
6	IBM	10	3%
7	Artifex Software	10	3%
8	PHP	9	3%
9	Drupal	5	2%
10	其他	151	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 21 个电信行业漏洞，16 个移动互联网行业漏洞，57 个工控系统行业漏洞（如下图所示）。其中，“Google Android 加密问题漏洞、Google Android MediaTek 权限提升漏洞、多款 Westermo 路由器欺骗漏洞、多款 Westermo 路由器硬编码密码漏洞、Cisco StarOS CLI 本地命令注入漏洞”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/>

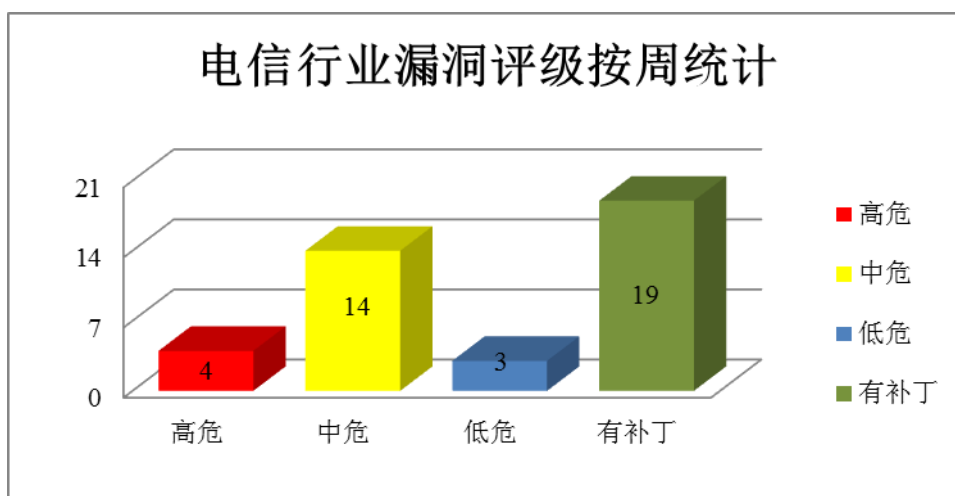


图 3 电信行业漏洞统计

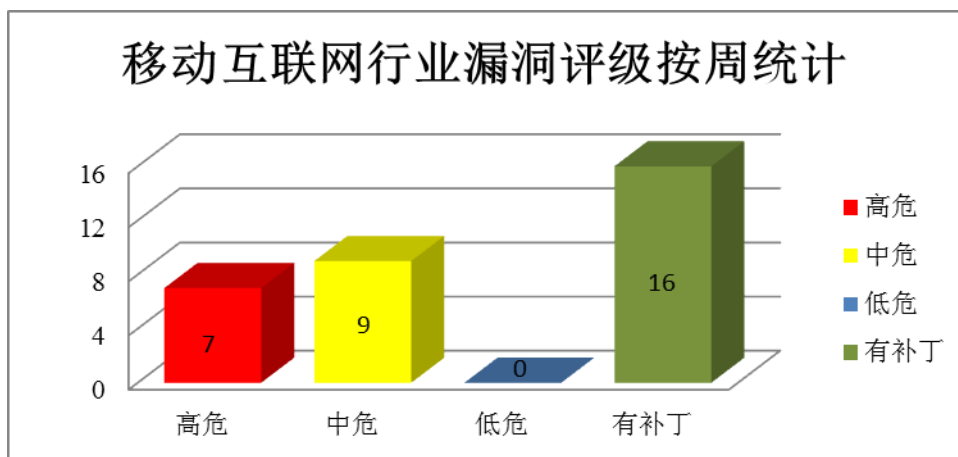


图 4 移动互联网行业漏洞统计

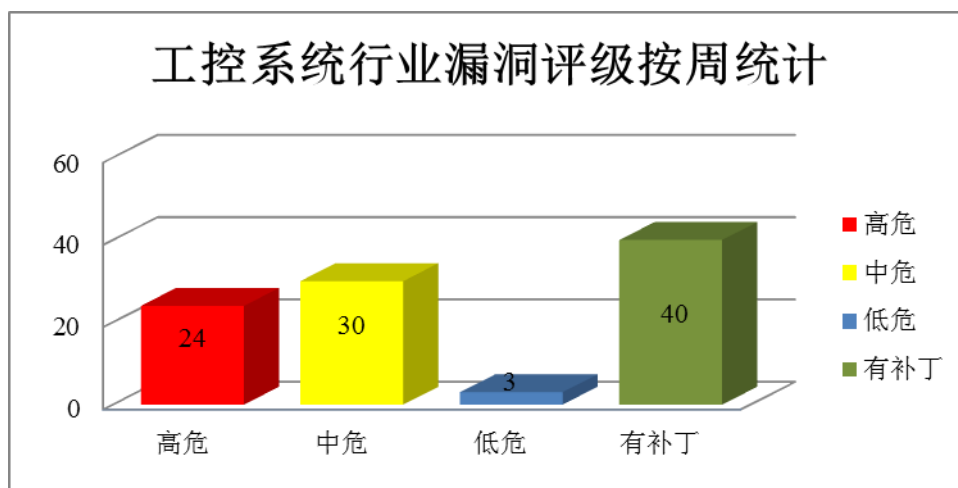


图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品，前者是一套 PDF 文件编辑和转换工具，后者是一套 PDF 文档阅读软件。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：Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2017-22670、CNVD-2017-22671、CNVD-2017-22672、CNVD-2017-22673、CNVD-2017-22674、CNVD-2017-22675、CNVD-2017-22741、CNVD-2017-22743）。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-2017-22670>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22671>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22672>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22673>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22674>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22675>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22741>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22743>

2、Cisco 产品安全漏洞

Cisco Elastic Services Controller 是美国思科（Cisco）公司的一个开源的模块化系统。Cisco Ultra Services Platform 是一个智能在线服务交付平台。Cisco ASR 5000 系列是一个用于部署高需求的 3G 网络以及向长期演进迁移的运营商级平台。Cisco ASR

5000 Series Aggregated Services Routers 是 ASR 5000 系列综合服务路由器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、绕过安全限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Elastic Services Controller 信息泄露漏洞（CNVD-2017-220967）、Cisco StarOS CLI 本地命令注入漏洞、Cisco Ultra Services Framework 信息泄露漏洞、Cisco Ultra Services Platform Elastic Services Controller Web 界面信息泄露漏洞、Cisco ASR 5000 Series Aggregated Services Routers StarOS 安全绕过漏洞、Cisco ASR 5000 Series Aggregated Services Routers StarOS 权限提升漏洞、Cisco ASR 5000 Series Aggregated Services Routers StarOS 任意文件写入漏洞、Cisco ASR 5500 Series Routers 拒绝服务漏洞。其中，“Cisco Elastic Services Controller 信息泄露漏洞（CNVD-2017-220967）、Cisco StarOS CLI 本地命令注入漏洞、Cisco Ultra Services Framework 信息泄露漏洞、Cisco Ultra Services Platform Elastic Services Controller Web 界面信息泄露漏洞”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-2017-22096>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22535>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22321>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22163>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22100>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22098>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22099>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22154>

3、Microsoft 产品安全漏洞

Microsoft Edge 是一款流行的 WEB 浏览器。Microsoft Internet Explorer 是一款流行的 WEB 浏览器。Microsoft Windows 是一款流行的计算机操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意的代码、泄露敏感信息或提升本地权限等。

CNVD 收录的相关漏洞包括：Microsoft EDGE 远程内存破坏代码执行漏洞、Microsoft EDGE 远程内存破坏代码执行漏洞（CNVD-2017-22681、CNVD-2017-22682）、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2017-22679）、Microsoft WordPad 远程代码执行漏洞、Microsoft Windows CLFS 本地权限提升漏洞、Microsoft Windows Explorer 拒绝服务漏洞、Microsoft Windows Https.sys 信息泄露漏洞。除“Microsoft Windows CLFS 本地权限提升漏洞、Microsoft Windows Explorer 拒绝服务漏洞、Microsoft Windows Https.sys 信息泄露漏洞”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-2017-22680>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22681>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22682>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22679>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22661>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22657>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22658>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22664>

4、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, Qualcomm 是使用在其中的一个高通组件。Broadcom Wi-Fi Driver 是使用在其中的一个 Wi-Fi 驱动模块。MediaTek networking driver 是使用在其中的一个网络连接驱动程序。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞提升权限或执行任意代码等。

CNVD 收录的相关漏洞包括: Google Android kernel 权限提升漏洞、Google Android MediaTek 权限提升漏洞、Google Android Qualcomm 组件存在未明漏洞 (CNVD-2017-22584)、Google AndroidBroadcom Wi-Fi 驱动程序提权漏洞、Google Android 存在未明漏洞 (CNVD-2017-22586)、Google Android 加密问题漏洞、Google Android Broadcom wi-fi 驱动器权限提升漏洞、Google Android 远程代码执行漏洞 (CNVD-2017-22360)。除“Google Android kernel 权限提升漏洞”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-2017-22356>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22355>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22584>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22541>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22586>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22585>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22542>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-22360>

5、NexusPHP SQL 注入漏洞

NexusPHP 是中国 Nexus 团队开发的一套使用 PHP 编写的资源分享社区解决方案。本周, NexusPHP 被披露存在 SQL 注入漏洞, 攻击者可利用漏洞执行任意的 SQL 命令。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-2017-22043>

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-2017-22089	Jython 任意代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://bugs.jython.org/issue2454
CNVD-2017-22323	Soffid IAM console 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.soffid.com/security-advisory1-update/
CNVD-2017-22341	Fedora Nagios package 设计缺陷漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://bugzilla.redhat.com/show_bug.cgi?id=1295446
CNVD-2017-22568	PCRE 'pcre_exec.c'本地拒绝服务漏洞	高	用户可联系供应商获得补丁信息： http://www.pcre.org/
CNVD-2017-22660	SQLite 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://sqlite.org/src/info/66de6f4a
CNVD-2017-22812	Philips' DoseWise Portal 明文存储漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://ics-cert.us-cert.gov/advisories/ICSMA-17-229-01
CNVD-2017-22813	Philips' DoseWise Portal 硬编码漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://ics-cert.us-cert.gov/advisories/ICSMA-17-229-01
CNVD-2017-22995	Apache Impala 身份验证绕过漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://issues.apache.org/jira/browse/IMPALA-5005
CNVD-2017-23006	多款 PDQ 产品权限获取漏洞	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.pdqinc.com/
CNVD-2017-23005	多款 PDQ 产品权限获取漏洞（CNVD-2017-23005）	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.pdqinc.com/

表 4 部分重要高危漏洞列表

小结：本周，Adobe 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

此外，Cisco、Microsoft、Google 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，NexusPHP 被披露存在 SQL 注入漏洞，攻击者可利用漏洞执行任意的 SQL 命令。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. 台达 PLC 编程软件 PMSOft 和 WPLSoft 爆出 11 个 0Day

台达是全球电源管理及散热方案的领导厂商，二十多年来，目前共设有广东东莞、江苏吴江、安徽芜湖、湖南郴州四个主要生产基地；二十三个研发中心。台达 PLC 编程软件 PMSOft 和 WPLSoft 爆出 11 个 0Day 漏洞，美国 ICS-CERT 已经获知漏洞情况，台达，这些 0Day 漏洞经过 120 天后，没有看到台达发布补丁，相关信息被公开。

参考链接：<http://toutiao.secjia.com/deltaww-pmsoft-wplsoft-0day?from=timeline&isappinstalled=0>

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