国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 05 月 15 日-2017 年 05 月 21 日 **2017 年第 21 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 440 个，其中高危漏洞 151 个、中危漏洞 263 个、低危漏洞 26 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 64 个（占 15%），其中互联网上出现“Invision Power Services Community Suite 跨站脚本漏洞、Trend Micro Threat Discovery Appliance 任意代码执行漏洞”等零日代码攻击漏洞。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 608 个，与上周（842）环比增下降 28%。

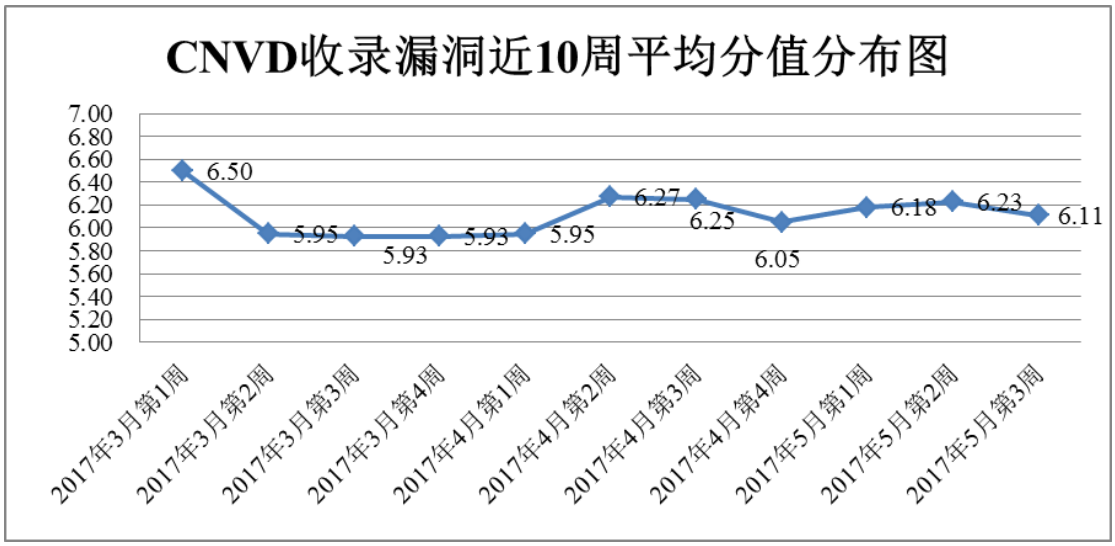

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 6 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 18 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 248 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 96 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 1

0 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

天津天地伟业数码科技有限公司、广州市毅航互联通信股份有限公司、延吉市先导高科技开发有限公司、金山软件股份有限公司、苏州烟火网络科技有限公司、苏州恩斯特网络科技有限公司、北京艾迈达斯科技有限公司、北京网御星云信息技术有限公司、锐捷网络股份有限公司、国电瑞驰远景信息技术(北京)有限公司、联想网御科技(北京)有限公司、德派软件（北京）有限公司、聚光科技（杭州）股份有限公司、北京中科汇联科技股份有限公司、北京全融信息服务有限公司、惠普公司、北京宽广智通信息技术有限公司、福建方维信息科技有限公司、devolo、趋势科技、HDWiki、Catfish CMS、鹏博士电信传媒集团-信息中心。

本周，CNVD 发布了《关于 Joomla! com_fields 组件存在 SQL 注入漏洞的情况公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4145

本周漏洞报送情况统计

本周，共 14 家成员单位、企业用户及个人用户报送了本周收录的全部 440 个漏洞。报送情况如表 1 所示。其中，东软、恒安嘉新、安天实验室、华为技术有限公司、天融信等单位报送数量较多。360 网神、漏洞盒子、江西安服信息产业有限公司、福建六壬网安股份有限公司、中新网络信息安全股份有限公司、安徽新华博信息技术股份有限公司、江苏君立华域信息安全技术有限公司、广州万方计算机科技有限公司、杭州朔方信息技术有限公司、上海零盾网络科技有限公司、山石网科通信技术有限公司、河北网信智安信息技术有限公司及其他个人白帽子向 CNVD 提交了 608 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	315	315
东软	273	0
恒安嘉新	143	0
安天实验室	128	0
华为技术有限公司	117	0
天融信	89	0

漏洞盒子	85	85
绿盟科技	53	0
H3C	38	0
中国电信集团系统集成有限责任公司	32	0
杭州安恒信息技术有限公司	25	0
厦门服云信息科技有限公司	12	1
北京数字观星科技有限公司	5	0
阿里云计算有限公司	3	0
江西安服信息产业有限公司	10	10
福建六壬网安股份有限公司	10	10
中新网络信息安全股份有限公司	8	8
安徽新华博信息技术股份有限公司	5	5
江苏君立华域信息安全技术有限公司	3	3
广州万方计算机科技有限公司	2	2
杭州朔方信息技术有限公司	2	2
上海零盾网络科技有限公司	2	2
山石网科通信技术有限公司	1	1
河北网信智安信息技术有限公司	1	1
CNCERT 山西分中心	16	16
CNCERT 宁夏分中心	5	5
CNCERT 北京分中心	2	2
CNCERT 河北分中心	2	2

CNCERT 吉林分中心	2	2
CNCERT 新疆分中心	2	2
CNCERT 广东分中心	2	2
个人	132	132
报送总计	1525	608
录入总计	440（去重）	608

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 440 个漏洞。其中应用程序漏洞 220 个， web 应用漏洞 74 个，操作系统漏洞 73 个，网络设备漏洞 34 个，安全产品漏洞 20 个，数据库漏洞 19 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	220
web 应用漏洞	74
操作系统漏洞	73
网络设备漏洞	34
安全产品漏洞	20
数据库漏洞	19

表 2 漏洞按影响类型统计表

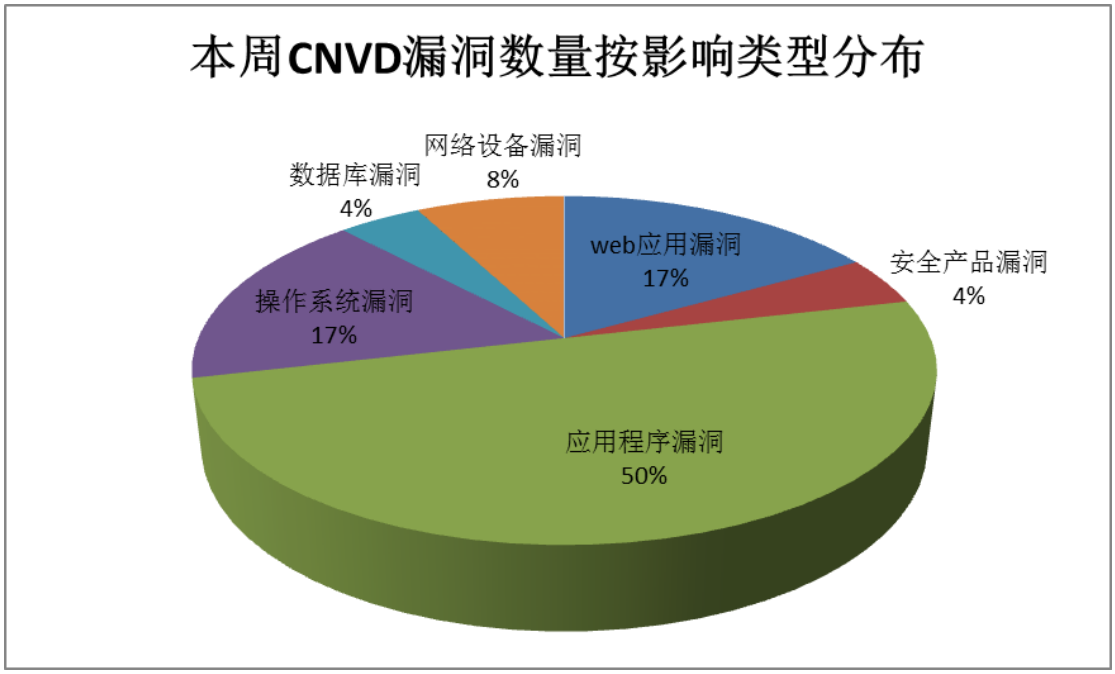

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Oracle、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	41	9%
2	Oracle	38	8%
3	Google	34	7%
4	Mozilla	25	6%
5	Apple	14	3%
6	WordPress	12	3%
7	Cisco	11	3%
8	Trend Micro	11	3%
9	Linux	11	3%
10	其他	243	55%

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 20 个电信行业漏洞，42 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图所示）。其中，“TP-Link TL-SG108E RC4 编码漏洞、TP-LINK C2 和 C20i 任意代码执行漏洞、Fortinet FortiGate/FortiOS 跨站脚本漏洞、BLF-Tech LLC VisualView HMI 本地代码执行漏洞、Rockwell Automation 远程拒绝服务漏洞、Mozilla Firefox for Android 存在未明漏洞（CNVD-2017-07066）、Apple iOS cryptographic API 调用验证漏洞、Google Android Qualcomm 声卡驱动程序权限提升漏洞”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/

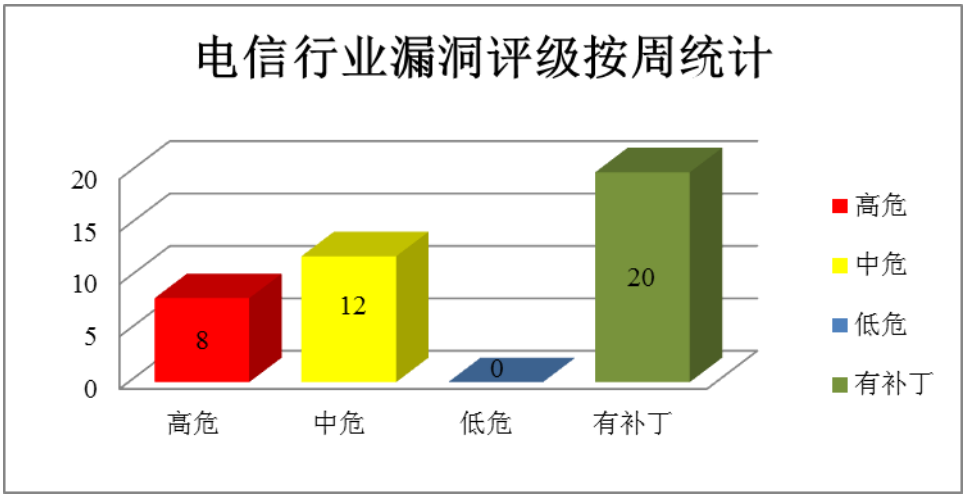

图 3 电信行业漏洞统计

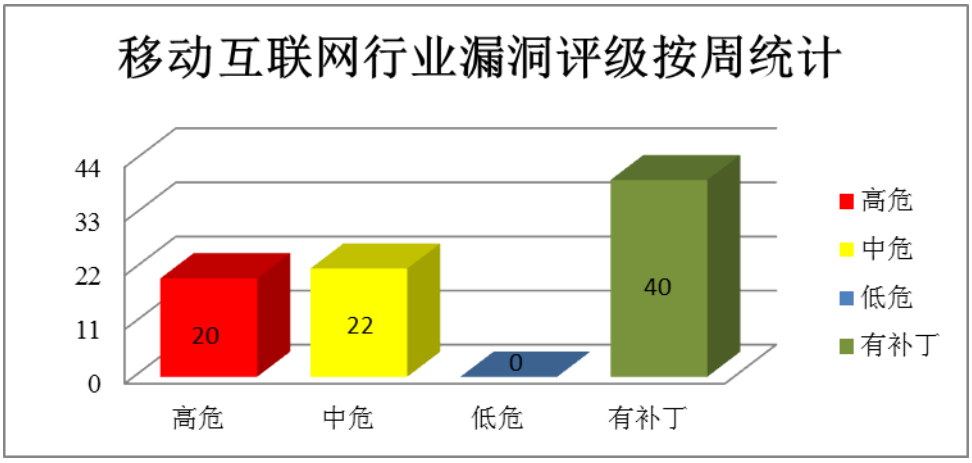

图 4 移动互联网行业漏洞统计

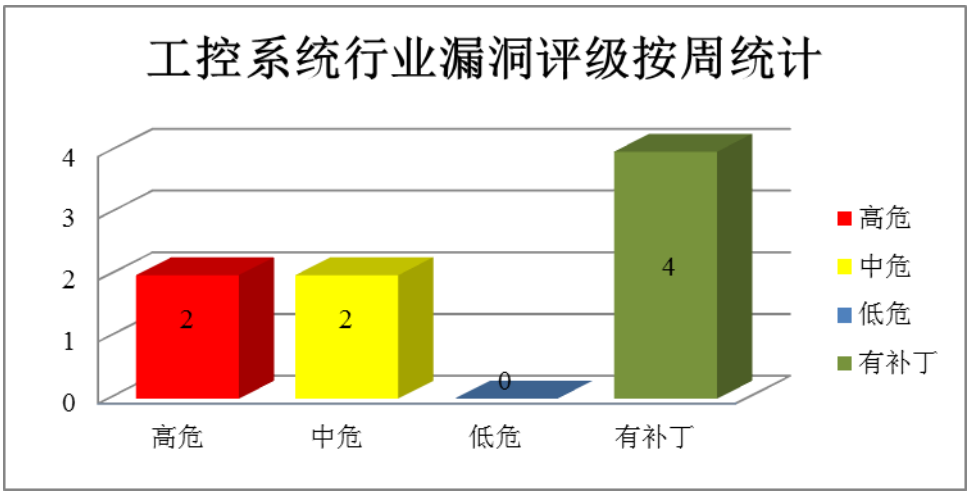

图 5 工控系统行业漏洞统计

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、Joomla! com_fields 组件存在 SQL 注入漏洞

Joomla!是美国 Open Source Matters 团队的一套使用 PHP 和 MySQL 开发的开源、跨平台的内容管理系统(CMS)。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞无需任何身份认证，获取数据库敏感信息。

CNVD 收录的相关漏洞包括：Joomla! com_fields 组件存在 SQL 注入漏洞。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-2017-06861

2、Microsoft 产品安全漏洞

Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。本周，该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 远程内存破坏漏洞（CNVD-2017-06589、CNVD-2017-06590、CNVD-2017-06591、CNVD-2017-06592、CNVD-2017-06593、CNVD-2017-06594、CNVD-2017-06595、CNVD-2017-06596）。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-2017-06589
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06590
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06591
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06592
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06593
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06594
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06595
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06596

3、Google 产品安全漏洞

Android 是一套以 Linux 为基础的开源操作系统。Mediaserver 是其中的一个多媒体服务组件。本周，该产品被披露存在远程代码执行和权限提升漏洞，攻击者可利用漏洞执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Google Android Mediaserver 权限提升漏洞（CNVD-2017-06807、CNVD-2017-06872、CNVD-2017-06873）、Google Android Mediaserver 远程代码执行漏洞（CNVD-2017-07090、CNVD-2017-07091、CNVD-2017-07092、CNVD-2017-07093、CNVD-2017-07094）。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-2017-06807
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06872

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06873
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07090
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07091
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07092
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07093
http://www.cnvd.org.cn/flaw/show/CNVD-2017-07094

4、Oracle 产品安全漏洞

Oracle Java SE 是美国甲骨文（Oracle）公司的一套标准版 Java 平台。Oracle E-Business Suite 是企业级商业应用的综合套装。Oracle Primavera Products Suite 是一款项目组合管理解决方案套件产品。Oracle Virtualization 是一套虚拟化解决方案。本周，上述产品被披露存在远程漏洞，攻击者可利用漏洞影响数据的可用性、保密性和完整性。

CNVD 收录的相关漏洞包括：Oracle Customer Interaction Histor 远程漏洞、Oracle Java SE AWT 远程漏洞、Oracle One-to-One Fulfillment 远程漏洞、Oracle Payables 远程漏洞、Oracle Primavera Gateway 远程漏洞、Oracle Primavera Gateway 远程漏洞（CNVD-2017-06627）、Oracle VM VirtualBox 远程漏洞（CNVD-2017-06471、CNVD-2017-06477）。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-2017-06467
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06469
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06466
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06465
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06473
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06627
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06471
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06477

5、Wordpress 插件 Organizer File 文件上传漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，WordPress 被披露存在文件上传漏洞，攻击者可利用该漏洞上传任意文件。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-2017-06849

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-201	Apple iOS 内核内存破坏漏洞	高	用户可参考如下厂商提供的安全补

7-06694	（CNVD-2017-06694）		丁以修复该漏洞：https://support.apple.com/zh-cn/HT207617
CNVD-2017-06695	Apple iOS cryptographic API 调用验证漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.apple.com/zh-cn/HT207617
CNVD-2017-06705	QEMU 权限许可和访问控制漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://wiki.qemu.org/Main_Page
CNVD-2017-06865	HP OpenCall Media Platform 远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.hp.com/
CNVD-2017-06905	TP-LINK C2 和 C20i 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://pierrekim.github.io/blog/2017-02-09-tplink-c2-and-c20i-vulnerable.html
CNVD-2017-06997	Dahua Technology Authentication 身份验证漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.dahua.com/
CNVD-2017-07020	Joomla com_tag 插件'tag'参数 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://downloads.joomla.org
CNVD-2017-07023	Portrait Displays SDK 本地权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.portrait.com/securityupdate.html
CNVD-2017-07026	Western Digital My Cloud 身份认证漏洞	高	用户可联系供应商获得补丁信息：https://www.wdc.com/products/personal-cloud-storage/my-cloud.htm
CNVD-2017-07040	Xen XENMEM_exchange 本地权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://xenbits.xen.org/xsa/advisory-212.html

表 4 部分重要高危漏洞列表

小结：本周，Joomla!被披露存在 SQL 注入漏洞，攻击者可利用漏洞无需任何身份认证，获取数据库敏感信息。此外，Microsoft 、Google、Oracle 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、提升权限或泄露敏感信息等。另外，WordPress 被披露存在文件上传漏洞，攻击者可利用该漏洞上传任意文件。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Trend Micro Threat Discovery Appliance 任意代码执行漏洞

验证描述

Trend Micro Threat Discovery Appliance（TDA）是美国趋势科技（Trend Micro）公司的一款集成云安全技术的威胁发现设备。

Trend Micro TDA 2.6.1062r1 及之前版本中的 admin_sys_time.cgi 文件存在安全漏洞。远程攻击者可借助 timezone 参数中的 shell 元字符利用该漏洞以 root 权限执行任意代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/142223/Trend-Micro-Threat-Discovery-Appliance-2.6.1062r1-admin_sys_time.cgi-Remote-Code-Execution.html

漏洞链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-06829

信息提供者

哈尔滨安天科技股份有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Joomla!3.7.0 SQL 注入攻击漏洞分析

Joomla 是一套世界第二流行的内容管理系统。Joomla 3.7 版本后引入一个新的组件“com_fields”，这一组件会引发易被利用的漏洞，并且不需要受害者网站上的高权限，这意味着任何人都可以通过对站点恶意访问利用这个漏洞。SQL 注入发生的本质是对请求数据过滤不严，因此攻击者在此有很多文章可以做——例如，泄露用户的密码哈希值（Hash）、登陆后的用户的会话控制（在第二种情况下，如果是获取到登陆后管理员的 session，那么整个网站的后台系统可能被控制）。

参考链接：http://www.freebuf.com/vuls/135035.html

2. 以网络摄像头为感染目标的新型 IoT 僵尸网络 Persirai

趋势科技（Trend Micro）最近发现了一种新型物联网（IoT）僵尸网络，该僵尸网络利用恶意软件 ELF_PERSIRAI.A 进行不断传播感染。据分析，目前已有多家原始设备制造商（OEM）的 1000 多种型号网络摄像头产品受此恶意网络感染，但趋势科技并未透露详细受影响制造商，下一步可能会和相关制造商配合进行感染识别和漏洞修复。这可能是继 Mirai 和 Hajime 之后又一波针对 IoT 设备的新型攻击力量，趋势科技把其命

名为 Persirai。中国是该类僵尸网络感染的重灾区，仅大陆地区的感染率就高达 20.3%。参考链接：http://www.freebuf.com/news/134512.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