

国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 08 月 01 日-2016 年 08 月 07 日

2016 年第 32 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 365 个，其中高危漏洞 183 个、中危漏洞 165 个、低危漏洞 17 个。漏洞平均分为 6.12 分。本周收录的漏洞中，涉及 0day 漏洞 166 个（占 45%）。其中互联网上出现“Cacti graph_view.php SQL 注入漏洞、TCCMSV9.0 最新版 SQL 注入漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 1282 个，与上周（158 个）相比增加 7.1 倍。

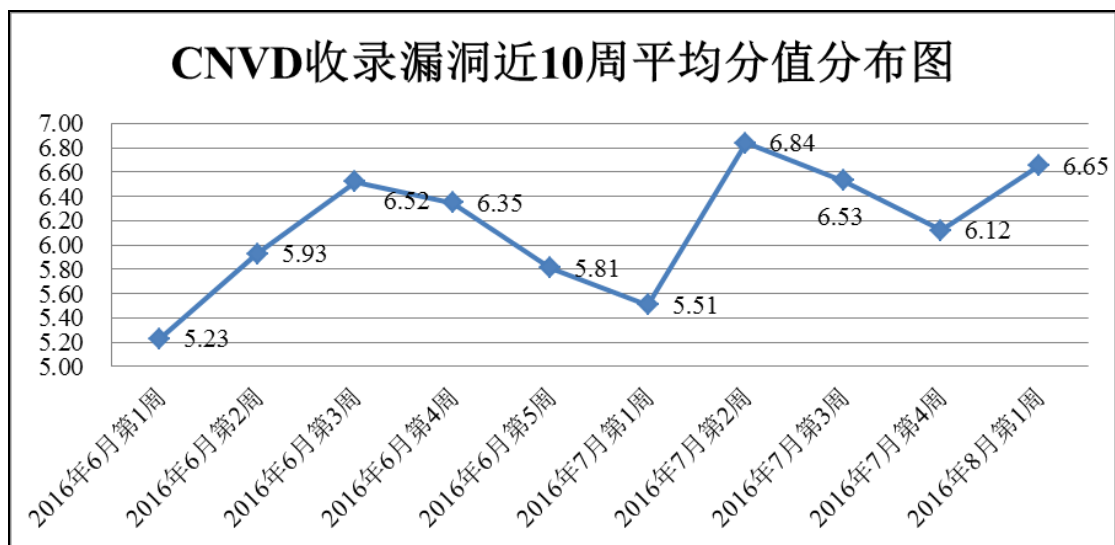


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 1 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 4 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 137 起，协调赛尔网络公司、上海交通大学网络信息中心等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 63 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 4 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：

北京图为先科技有限公司、济南昂利万软件开发有限公司、中国铁建股份有限公司、太原迅易科技有限公司、深圳市金伦科技有限公司、中国电子学会、catdvi、中国资本市场标准网、中煤地质新闻网、财报网、分析化学网站。

本周漏洞报送情况统计

本周，共 9 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 365 个漏洞。报送情况如表 1 所示。其中，奇虎（补天平台）、启明星辰、安天实验室、绿盟科技等单位报送数量较多。补天平台、漏洞盒子、High-Tech Bridge Security Research Lab 及其他个人白帽子向 CNVD 提交了 1282 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
奇虎（补天平台）	1185	1185
启明星辰	200	0
安天实验室	174	0
绿盟科技	111	0
天融信	92	0
恒安嘉新	70	2
杭州安恒信息技术有限公司	68	0
中国电信集团系统集成有限责任公司	49	0
H3C	47	0
漏洞盒子	54	54
CNCERT 江西分中心	8	8
CNCERT 宁夏分中心	3	3
CNCERT 上海分中心	2	2
CNCERT 天津分中心	1	1

High-Tech Bridge Security Research Lab	1	1
个人	26	26
报送总计	2091	1282
录入总计	365（去重）	1282

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 365 个漏洞。其中应用程序漏洞 141 个，web 应用漏洞 123 个，操作系统漏洞 66 个，网络设备漏洞 22 个，安全产品漏洞 8 个，数据库漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	141
web 应用漏洞	123
操作系统漏洞	66
网络设备漏洞	22
安全产品漏洞	8
数据库漏洞	5

表 2 漏洞按影响类型统计表

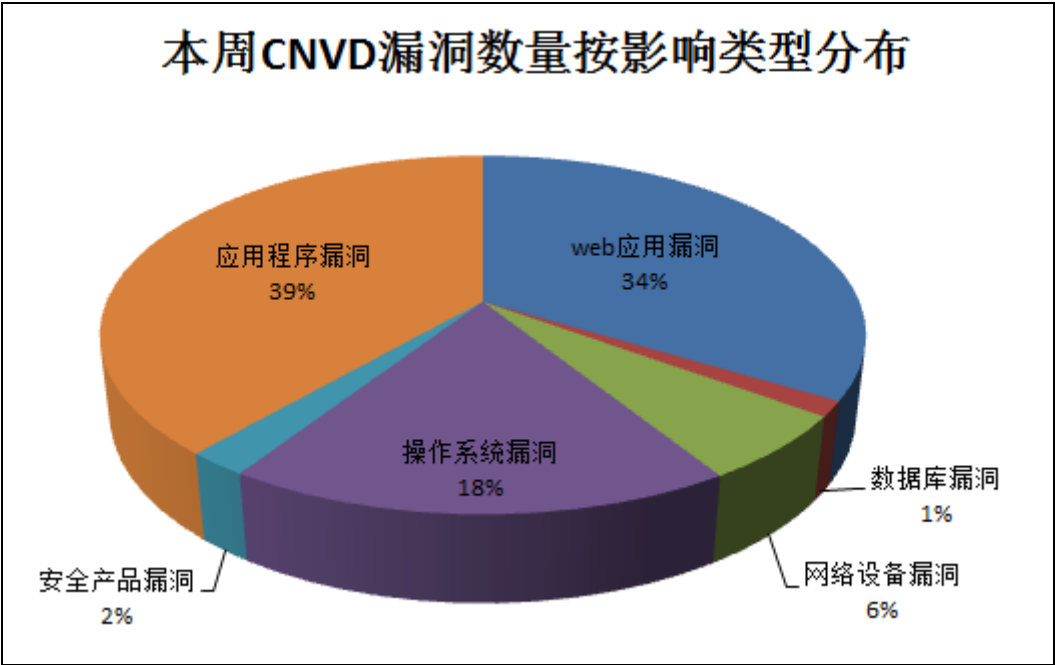


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、IBM、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	Apple	46	13%
2	IBM	17	5%
3	Google	15	4%
4	Wireshark	11	3%
5	SAP	10	3%
6	Wordpress	6	2%
7	Linux	6	2%
8	Joomla!	6	2%
9	Crestron Electronics	6	2%
10	其他	242	64%

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 个电信行业漏洞，39 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，“多款 Apple 产品 libxslt 内存破坏拒绝服务漏洞、多款 Apple 产品 libxslt 内存破坏拒绝服务漏洞（CNVD-2016-05769、CNVD-2016-05749、CNVD-2016-05739）、多款 Apple 产品 libxml2 内存破坏拒绝服务漏洞（CNVD-2016-05743、CNVD-2016-05742、CNVD-2016-05741）、Google Nexus 权限提升漏洞（CNVD-2016-06073、CNVD-2016-06072、CNVD-2016-06071）等”的综合评级为“高危”。详情请参照 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/>

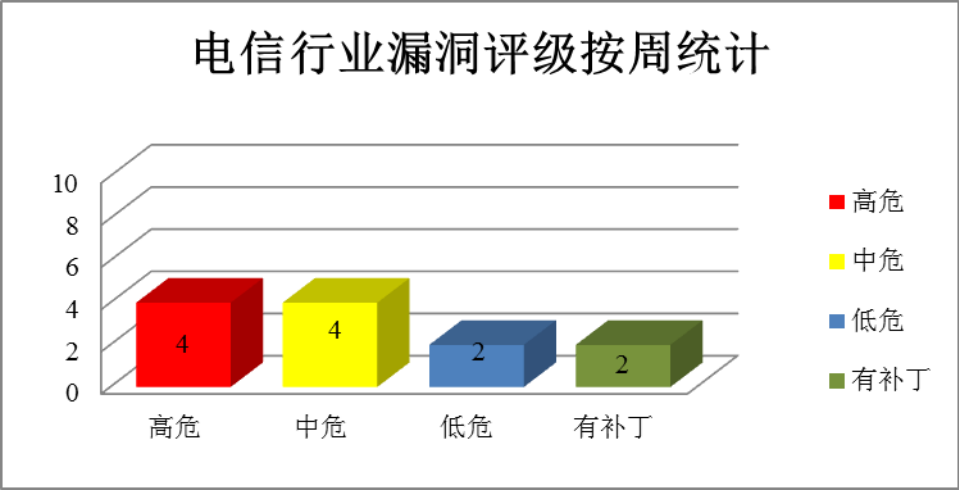


图 3 电信行业漏洞统计

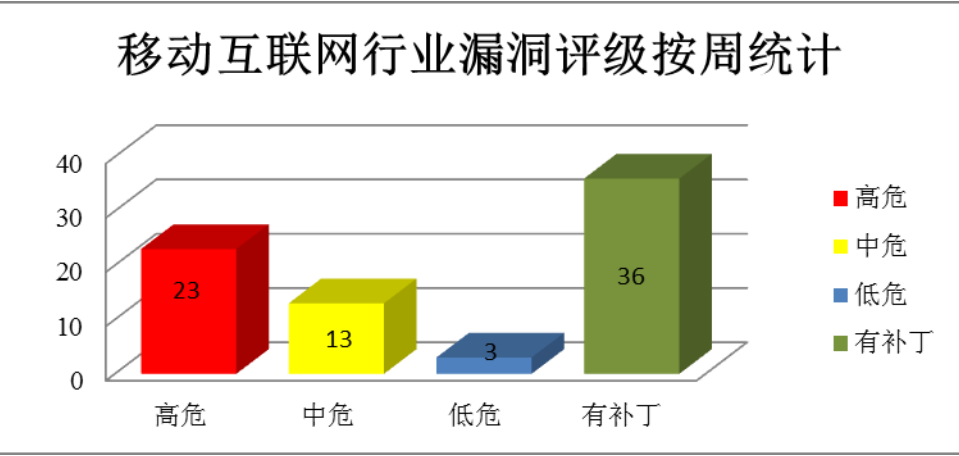


图 4 移动互联网行业漏洞统计

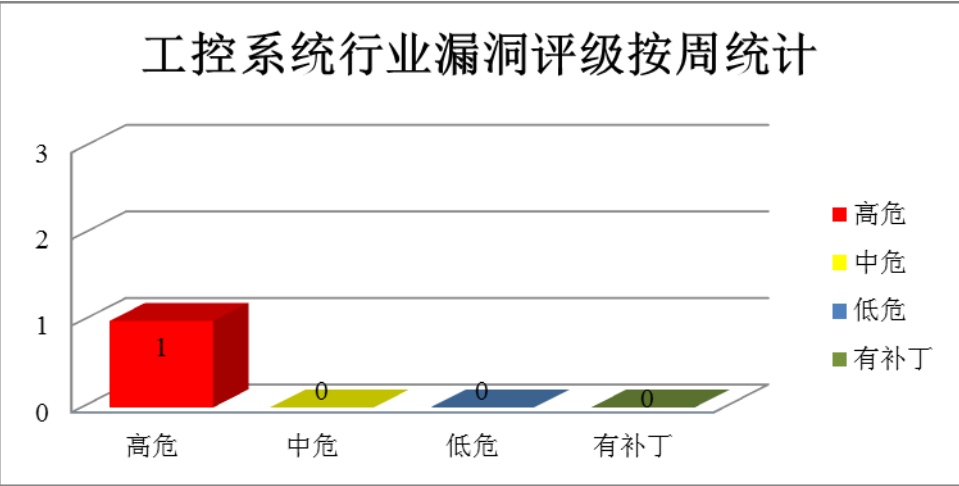


图 5 工控系统行业漏洞统计



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、Apple 产品安全漏洞

Apple OS X 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统。QuickTime 是其中的一个多媒体播放组件。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，或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple OS X QuickTime 内存破坏漏洞（CNVD-2016-05729、CNVD-2016-05730、CNVD-2016-05731、CNVD-2016-05732、CNVD-2016-05733、CNVD-2016-05736、CNVD-2016-05737）、Apple OS X Login Window 内存破坏漏洞（CNVD-2016-05758）等。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-2016-05729>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05730>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05731>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05732>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05733>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05736>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05737>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05758>

2、IBM 产品安全漏洞

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案，IBM AIX（Advanced Interactive eXecutive）是一套 UNIX 操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM SQL 注入漏洞、IBM QRadar SIEM 跨站脚本漏洞、IBM QRadar SIEM 跨站请求伪造漏洞、IBM QRadar SIEM 命令注入漏洞、IBM QRadar SIEM 未授权访问漏洞、IBM QRadar SIEM 信息泄露漏洞（CNVD-2016-05955）、IBM AIX 信息泄露漏洞、IBM AIX 远程拒绝服务漏洞等。其中，“IBM QRadar SIEM SQL 注入漏洞、IBM QRadar SIEM 命令注入漏洞”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-2016-05950>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05953>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05948>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05954>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05952>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05955>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05817>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05854>

3、Google 产品安全漏洞

Google Nexus 是谷歌公司搭载原装 Android 系统的高端手机系列，Google Android 是美国谷歌（Google）公司和开放手机联盟领导及开发的基于 Linux 开放性内核的移动操作系统。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：Google Nexus 权限提升漏洞（CNVD-2016-06077、CNVD-2016-06075、CNVD-2016-06074、CNVD-2016-06073、CNVD-2016-06072、CNVD-2016-06071、CNVD-2016-06076）、Google Android 权限提升漏洞等。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-2016-06077>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06075>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06074>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06073>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06072>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06071>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06076>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06070>

4、Wireshark 产品安全漏洞

Wireshark（前称 Ethereal）是 Wireshark 团队开发的一套网络数据包分析软件。该软件的功能是截取网络数据包，并显示出详细的数据以供分析。本周，该产品被披露存在远程拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Wireshark 'add_capabilities()'函数远程拒绝服务漏洞、Wireshark CORBA IDL Dissector 远程拒绝服务漏洞、Wireshark MMSE Dissector 远程拒绝服务漏洞、Wireshark NDS Dissector 远程拒绝服务漏洞、Wireshark OpenFlow 解析器远程拒绝服务漏洞、Wireshark RLC Dissector 拒绝服务漏洞、Wireshark RLC Dissector 远程拒绝服务漏洞、Wireshark WBXML Dissector 远程拒绝服务漏洞等。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-2016-05723>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05872>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05873>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05724>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05726>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05871>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05728>

5、Cacti graph_view.php SQL 注入漏洞

Cacti 是 Cacti 集团的一套开源的网络流量监测和分析工具。本周，Cacti graph_view.php 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意 SQL 命令。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序。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-2016-05904>

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-2016-05825	DBD::mysql 'my_login()'远程代码执行漏洞	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： https://github.com/perl5-dbi/DBD-mysql/pull/45/files
CNVD-2016-05822	Atlassian Bamboo 远程代码执行漏洞	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： https://jira.atlassian.com/browse/BAM-17736?src=confmacro&_ga=1.65705644.34970059.1459525314
CNVD-2016-05840	NetBSD 本地提权漏洞	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://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2016-006.txt.asc
CNVD-2016-05851	PHP Gettext 远程代码执行漏洞	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： https://launchpad.net/php-gettext/
CNVD-2016-05848	Centreon Web 界面远程命令执行漏洞	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： https://www.centreon.com/
CNVD-2016-05862	Wordpress Event-Registration 插件存在多个漏洞	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： https://wordpress.org/
CNVD-2016-05859	WordPress Ultimate-Product-Catalog 插件 SQL 注入漏洞	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://www.wordpress.org/
CNVD-2016-05947	Rockwell Automation FactoryTalk EnergyMetrix 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，详情请关注厂商主页： http://www.rockwellautomation.com/
CNVD-2016-05937	Crestron Electronics DM-TXRX-100-STR 硬编码密码漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://www.crestron.com/downloads/pdf/spec_sheets/commercial_and_residential/dm-txrx-100-str.pdf
CNVD-2016-05941	Crestron Electronics DM-TXRX-100-STR 安全限制绕过漏洞（CNVD-2016-05941）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://www.crestron.com/downloads/pdf/spec_sheets/commercial_and_residential/dm-txrx-100-str.pdf

表 4 部分重要高危漏洞列表

小结：本周，Apple 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，或发起拒绝服务攻击。此外，IBM、Google、Wireshark 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击和发起拒绝服务攻击等。另外，Cacti graph_view.php 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意 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、Novell Filr 命令注入漏洞

验证描述

Novell Filr 是美国 Novell 公司的一套用于企业的文件访问和共享解决方案。

Novell Filr 1.2 Security Update 2 及之前的版本和 2.0 Security Update 1 及之前的版本中的 vaconfig/time 文件中存在操作系统命令注入漏洞。远程攻击者可通过 ntpServer 参数中的 shell 元字符利用该漏洞执行任意命令。

验证信息

POC 链接：<http://seclists.org/bugtraq/2016/Jul/119>

漏洞链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05960>

信息提供者

恒安嘉新（北京）科技有限公司

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. Adobe Flash Player 漏洞 (CVE-2016-4117) 样本分析

今年五月份，国外安全专家发现了一个未知的 Adobe 漏洞被利用。在该漏洞被披露后，Adobe 发布了一个升级补丁用于修复此漏洞 (APSB16-15)，编号为 CVE-2016-4117。同时，CVE-2016-4117 漏洞被列为高危漏洞，在 CVSS Score 中被评为 10.0，它同时影响到 Windows, Mac OS X, Linux 和 Chrome OS。利用该漏洞可能会导致系统崩溃，甚至攻击者可以控制受影响的系统。

参考链接: <http://www.freebuf.com/vuls/110707.html>

2. HTTP2.0 协议被曝 4 个高危漏洞，可致服务器崩溃

去年 2 月，谷歌把自家的 SPDY 项目捆绑进 HTTP2.0，意在加强网页加载速度和用户的在线浏览体验。三个月后 HTTP2.0 正式发布，HTTP2.0 如今已成为大部分网站最主要的 HTTP 协议版本。来自 Imperva 的几位安全专家在 Black Hat 大会上公布了至少 4 个高危漏洞，慢速连接攻击 (CVE-2016-1546)、HPACK BOMB (CVE-2016-1544, CVE-2016-2525)、依赖循环攻击 (CVE-2015-8659)、数据流多路复用 (CVE-2016-0150) 漏洞。允许攻击者通过传输千兆级别的数据有效载荷到目标服务器，导致服务器无限循环，使 Web 服务器的处理速度变慢，甚至瘫痪。

参考链接: <http://www.freebuf.com/news/111111.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