国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 05 月 02 日-2016 年 05 月 08 日　　2016 年第 19 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 132 个，其中高危漏洞 28 个、中危漏洞 88 个、低危漏洞 16 个。漏洞平均分值为 5.63 分。本周收录的漏洞中，涉及 0day 漏洞 21 个（占 16%）。其中互联网上出现“BaumerVeriSens Application Suite 缓冲区溢出漏洞、Gemtek CPE7000/WLTCS-106 存在多个漏洞”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。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 1330 个，与上周（1604 个）环比下降 17%，但较前五周比，事件型漏洞数量仍然处于高位。根据近期监测结果，针对 Apache Struts 2 S2-032 漏洞以及以往版本远程代码执行漏洞、ImageMagick 远程代码执行漏洞诱发了大规模攻击和扫描尝试，互联网站面临较高的安全风险并已出现较多威胁实例。本周漏洞威胁评价为“高”。

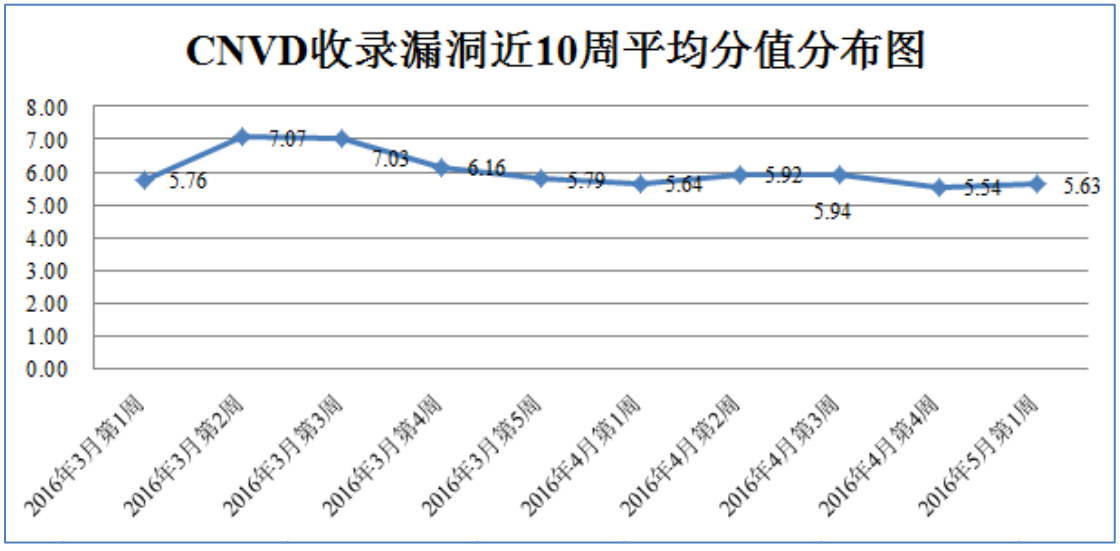

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及个人报送了本周收录的全部 132 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、安恒信息等单位报送数量较多。补天平台、乌云、漏洞盒子、西安四叶草信息技术有限公司、白帽子向 CNVD 提交了 1330 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)	853	853
启明星辰	140	0
安天实验室	121	0
杭州安恒信息技术有限公司	78	0
天融信	71	0
恒安嘉新	63	1
中国电信集团系统集成有限责任公司	49	0
绿盟科技	38	0
H3C	8	0
东软	148	0
乌云	271	271
漏洞盒子	45	45
腾讯电脑管家	8	8
西安四叶草信息技术有限公司	130	130
CNCERT 安徽分中心	3	3
CNCERT 宁夏分中心	3	3
个人	16	16
报送总计	2045	1330

录入总计	132（去重）	1330

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 132 个漏洞。其中应用程序漏洞 103 个，操作系统漏洞 22 个，Web 应用漏洞 5 个，网络设备漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	103
操作系统漏洞	22
web 应用漏洞	5
网络设备漏洞	2

表 2 漏洞按影响类型统计表

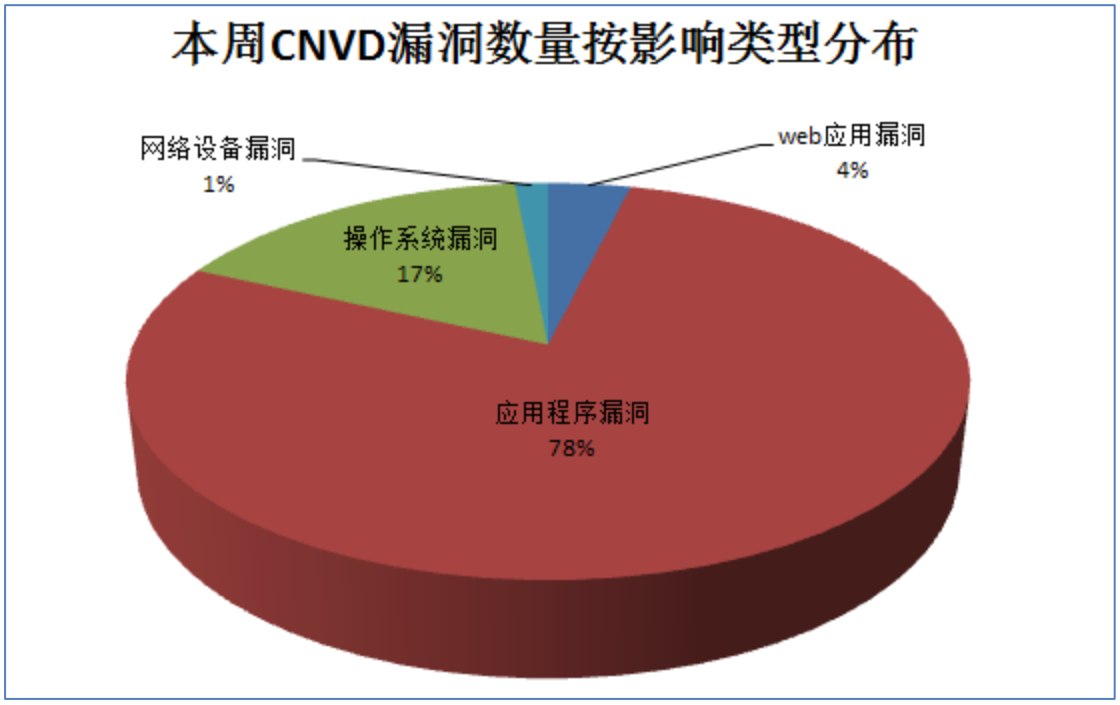

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、Mozilla、PHP 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	Linux	22	17%
2	Mozilla	14	11%
3	PHP	13	10%
4	ntpd	9	7%

5	Wireshark	7	5%
6	OpenSSL	6	5%
7	Foxit	6	5%
8	Cisco	4	3%
9	IBM	3	2%
10	其他	48	35%

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 4 个电信行业漏洞（如下图所示）。其中，“SystechSysLINK M2M Modular Gateway 权限获取漏洞（CNVD-2016-02708）”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/

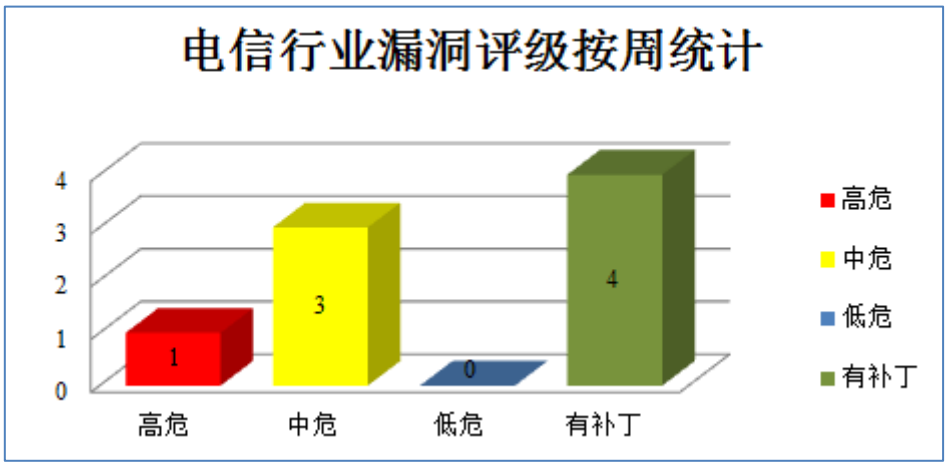

图 3 电信行业漏洞统计

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、 OpenSSL 产品安全漏洞

近日，OpenSSL 发布了安全公告，共含 6 项更新。其中 2 项更新的综合评级为“高危”。本周，CNVD 收录了对应的漏洞，远程攻击者利用漏洞可导致程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：OpenSSL EBCDIC 越界读漏洞、OpenSSL ASN.1 BIO 内存过度分配漏洞、OpenSSLEVP_EncodeUpdate 溢出漏洞（CNVD-2016-02678）、OpenSSLEVP_EncodeUpdate 溢出漏洞、OpenSSL 密文填塞漏洞、OpenSSL ASN.1 encoder 内存破坏漏洞。其中，“OpenSSL 密文填塞漏洞、OpenSSL ASN.1 encoder 内存破坏漏洞”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-2016-02676

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02677

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02678

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02679

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02680

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02681

2、 ImageMagick 产品安全漏洞

本周，CNVD 收录了 ImageMagick 远程代码执行漏洞（CNVD-2016-02721，对应 CVE-2016-3714）。远程攻击者利用漏洞通过上传恶意构造的图像文件，可在目标服务器执行任意代码，进而获得网站服务器的控制权。由于有多种编程语言对 ImageMagick 提供调用支持且一些广泛应用的 Web 中间件在部署中包含相关功能，对互联网站安全构成重大威胁。

CNVD 收录的相关漏洞包括：ImageMagick 远程代码执行漏洞。上述漏洞的综合评级为“高危”。目前，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-2016-02721

3、 Mozilla 产品安全漏洞

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Mozilla Maintenance Service 是其中的一个静默升级程序组件。本周，上述产品被披露存在多个安全漏洞，远程攻击者可利用漏洞获取敏感信息、绕过权限限制、进行跨站脚本攻击或执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 权限绕过漏洞、Mozilla Firefox 信息泄露漏洞（CNVD-2016-02763）、Mozilla Firefox 跨站脚本漏洞（CNVD-2016-02671）、Mozilla Firefox 内存错误引用漏洞（CNVD-2016-02672）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2016-02688）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞、Mozilla Firefox ESR 内存破坏漏洞、Mozilla Firefox 内存破坏漏洞（CNVD-2016-02690）等。上述漏洞中，除“Mozilla Firefox 权限绕过漏洞、Mozilla Firefox 信息泄露漏洞（C

NVD-2016-02763）、Mozilla Firefox 跨站脚本漏洞（CNVD-2016-02671）”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-2016-02764

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02763

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02671

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02672

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02688

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02687

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02689

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02690

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，上述产品被披露存在拒绝服务、权限获取和任意文件读取漏洞，允许攻击者利用漏洞获取权限、读取任意文件和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2016-02787）、Linux kernel 权限获取漏洞、Linux kernel 拒绝服务漏洞（CNVD-2016-02768）、Linux kernel 权限获取漏洞（CNVD-2016-02786）、Linux kernel 任意文件读取漏洞、Linux kernel 争用条件拒绝服务漏洞（CNVD-2016-02777）、Linux kernel 拒绝服务漏洞（CNVD-2016-02789）、Linux kernel 拒绝服务漏洞（CNVD-2016-02788）等。其中，“Linux kernel 拒绝服务漏洞（CNVD-2016-02787）、Linux kernel 权限获取漏洞、Linux kernel 拒绝服务漏洞（CNVD-2016-02768）”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-2016-02787

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02792

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02768

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02786

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02797

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02777

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02789

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02788

5、WPS Office 内存破坏漏洞

Kingsoft WPS Office 是一款办公软件套件，常用组件包括：Writer、Spreadsheets 和

Presentation 等。本周，WPS Office 被披露存在内存破坏漏洞，允许攻击者利用该漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。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-2016-02730

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-2016-02696	PHPBack SQL 注入漏洞	高	无
CNVD-2016-02695	Gemtek CPE7000/WLTCS-106 存在多个漏洞	高	无
CNVD-2016-02693	WEG SuperDrive G2 权限提升漏洞	高	无
CNVD-2016-02708	SystechSysLINK M2M Modular Gateway 权限获取漏洞（CNVD-2016-02708）	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.systech.com/
CNVD-2016-02717	多款 Adobe 产品内存错误引用漏洞（CNVD-2016-02717）	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2016-02751	Cisco WebEx Productivity Tools 搜索路径处理漏洞	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.webex.com/
CNVD-2016-02731	Foxit Reader PDF 解析内存破坏漏洞	高	无
CNVD-2016-02726	Google Chrome pdfium 堆内存错误引用漏洞	高	无
CNVD-2016-02724	BaumerVeriSens Application Suite 缓冲区溢出漏洞	高	无
CNVD-2016-02723	Adobe Flash 任意代码执行漏洞	高	无

表 4 部分重要高危漏洞列表

小结：近日，OpenSSL 发布了安全公告，共含 6 项更新。其中 2 项更新的综合评级为“高危”。远程攻击者利用漏洞可导致程序崩溃，执行任意代码；ImageMagick 被披露存在远程代码执行漏洞，远程攻击者利用漏洞通过上传恶意构造的图像文件，可在目标服务器执行任意代码，进而获得网站服务器的控制权。此外，Mozilla、Linux 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获取权限、进行跨站脚本和发起拒绝服务攻击等。另外，WPS Office 被披露存在一个高危漏洞，允许攻击者利用该漏洞构

建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。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. 三星 SmartThings 平台被爆新漏洞，可触发火灾报警器

研究人员发现三星 SmartThings 平台存在多个漏洞，利用软件漏洞可以解锁车门，未经主人允许可以设置新的虚拟按键，通过虚假的信息设置打开了智能锁，甚至还可以通过发送虚假信息触发火灾报警器以及关闭度假模式（主人离开后自动调节照明和安全的设置）等。目前，SmartThings 首席执行官 AlexHawkinson 第一时间作出了回应，表示这个漏洞已经被修复，同时已经开始与密歇根大学的团队合作找到更多潜在的漏洞。

参考链接：http://www.freebuf.com/news/103348.html

2. Android 恶意软件又出新招：伪装 Google Chrome 升级，窃取银行卡数据

对于 Android 用户而言，使用 Android 设备已经变成充满危机的行为，因为平均每天都会曝出针对 Android 系统的新型恶意软件。这一次，Android 恶意软件又出新招了。一个看起来无害的 Google Chrome 移动版本的升级，实际上是一种恶意软件，目的是窃取用户的财务信息和其他个人私密数据等。该恶意软件托管的页面也被设计的看起来就像是 Android 或谷歌的官方网页一样，让用户防不胜防。该恶意软件通过提醒用户 2015 年出现的 CTB Locker 以及 Critroni 勒索软件的危害，诱骗用户下载伪造的 Google Chrome 升级，进而盗窃用户数据。目前，该恶意软件已经被 Zscaler——一家安全公司发现，根据他们的研究发现：这个恶意软件功能十分强大，它可以监控通话记录，追踪短信信息，检索浏览器历史记录，而最具危害性的是，它还可以窃取用户银行信息。

参考链接：http://www.freebuf.com/news/103403.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