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 09 日-2016 年 05 月 15 日　　2016 年第 20 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 278 个，其中高危漏洞 112 个、中危漏洞 152 个、低危漏洞 14 个。漏洞平均分值为 6.59 分。本周收录的漏洞中，涉及 0day 漏洞 20 个（占 7%）。其中互联网上出现“File Hub 任意文件上传漏洞”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 1185 个，与上周（1330 个）环比下降 11%。

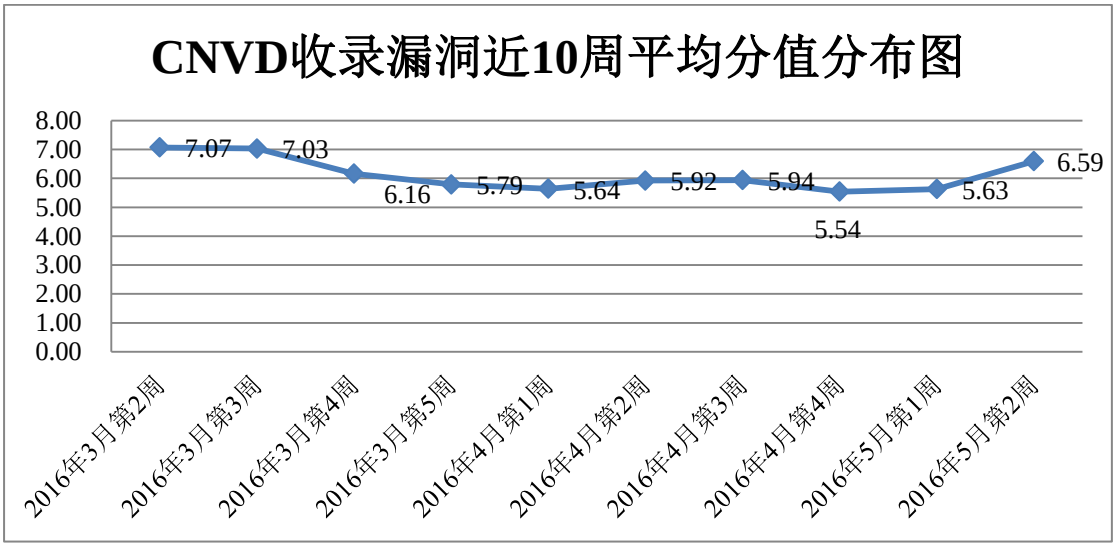

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 278 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、上海云盾信息技术有限公司、广州白狐网络科技有限公司、福

建六壬网安股份有限公司及白帽子向 CNVD 提交了 1185 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)	571	571
乌云	552	552
天融信	252	0
安天实验室	233	0
启明星辰	206	0
恒安嘉新	111	1
中国电信集团系统集成有限责任公司	101	13
绿盟科技	98	0
杭州安恒信息技术有限公司	60	0
漏洞盒子	23	23
H3C	6	0
腾讯玄武实验室	1	0
福建六壬网安股份有限公司	3	3
上海云盾信息技术有限公司	1	1
广州白狐网络科技有限公司	2	2
CNCERT 江西分中心	1	1
CNCERT 福建分中心	1	1
个人	17	17
报送总计	2239	1185
录入总计	278（去重）	1185

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 278 个漏洞。其中应用程序漏洞 180 个，操作系统漏洞 62 个，Web 应用漏洞 16 个，网络设备漏洞 13 个，安全产品漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	180
操作系统漏洞	62
web 应用漏洞	16
网络设备漏洞	13
安全产品漏洞	7

表 2 漏洞按影响类型统计表

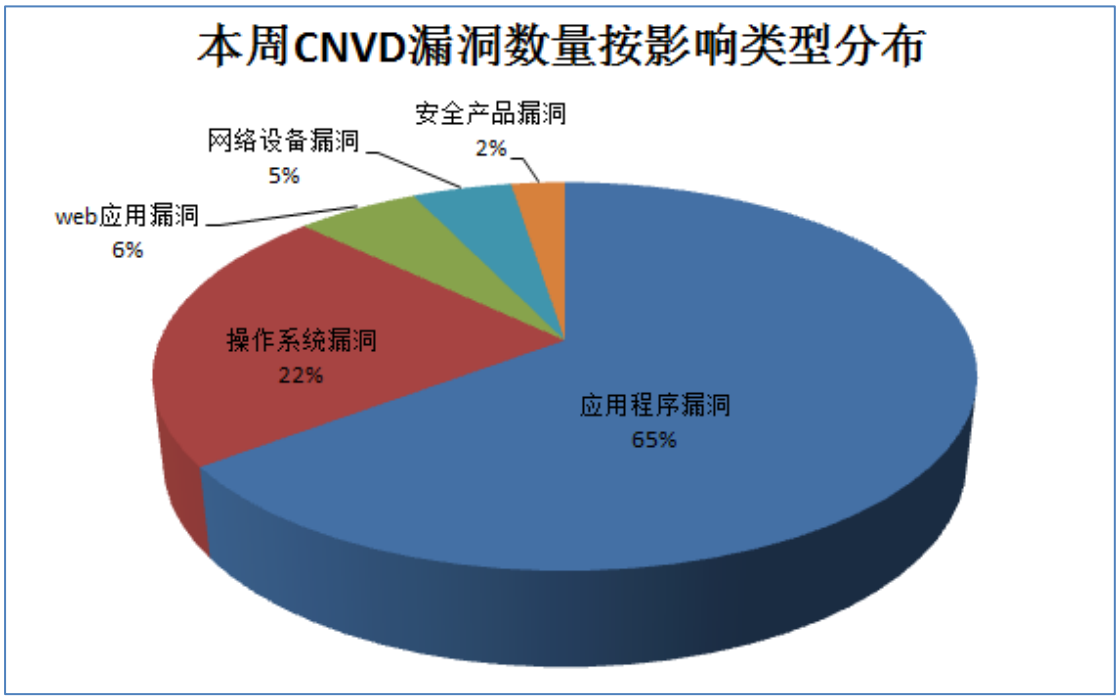

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、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。

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	50	18%
2	Google	42	15%
3	Microsoft	33	12%
4	PHP	11	4%
5	IBM	10	4%
6	GNU	8	3%
7	HP	6	2%

8	Cisco	5	2%
9	Symantec	4	1%
10	其他	109	39%

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 6 个电信行业漏洞，41 个移动互联网行业漏洞（如下图所示）。其中，“HELP NetCommWireless HSPA 3G10WVE 命令注入漏洞、HELP NetCommWireless HSPA 3G10WVE 安全绕过漏洞、Android Qualcomm TrustZone 权限提升漏洞（CNVD-2016-02834、CNVD-2016-02835）、Android NVIDIA Video Driver 权限提升漏洞（CNVD-2016-02826、CNVD-2016-02827、CNVD-2016-02828、CNVD-2016-02829）、Android Debuggerd 权限提升漏洞、Android Mediaserver 任意代码执行漏洞（CNVD-2016-02841、CNVD-2016-02842）、Android NVIDIA Video Driver 权限提升漏洞（CNVD-2016-02803、CNVD-2016-02804）、Android Qualcomm MDP Driver 提权漏洞、Android Qualcomm Buspm Driver 提权漏洞（CNVD-2016-02838、CNVD-2016-02839）、Android Binder 权限提升漏洞、Android Bluetooth 任意代码执行漏洞、Android kernel 任意代码执行漏洞、Android MediaTek Wi-Fi Driver 提权漏洞、Android Mediaserver 提权漏洞（CNVD-2016-02848、CNVD-2016-02849、CNVD-2016-02847、CNVD-2016-02846、CNVD-2016-02845）、Android Wi-Fi 提权漏洞、Android NVIDIA Video Driver 提权漏洞（CNVD-2016-02832）”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/

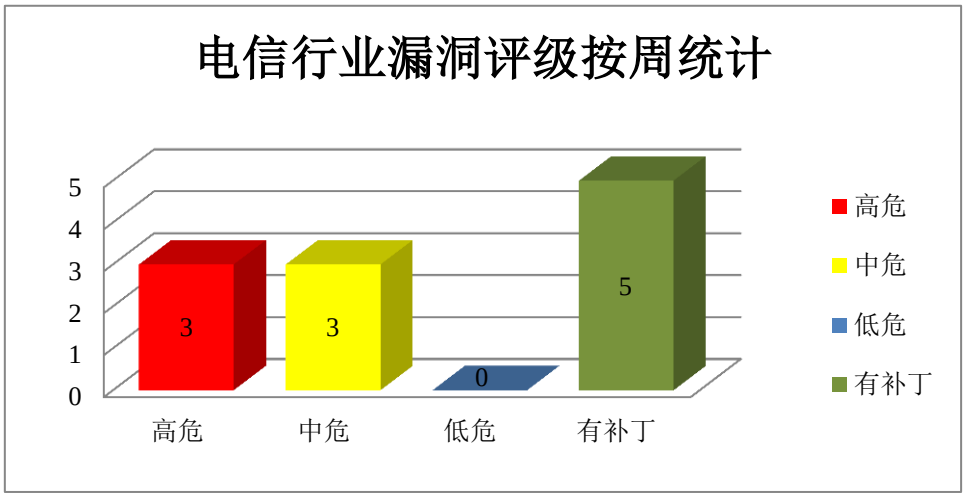

图 3 电信行业漏洞统计

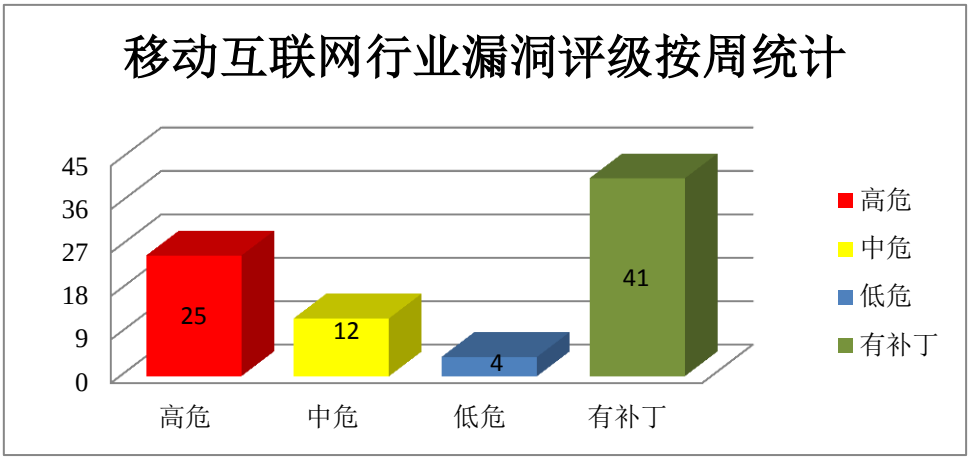

图 4 移动互联网行业漏洞统计

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、 Microsoft 产品安全漏洞

5 月 10 日，微软发布了 2016 年 5 月份的月度例行安全公告，共含 16 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Server、Office、Office Service、Web Apps、和.NET Framework 中存在的 36 个安全漏洞。其中，8 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2016-03117、CNVD-2016-03118）、Microsoft JScript 和 VBScript 脚本引擎内存破坏漏洞（CNVD-2016-03119）、Microsoft Chakra JavaScript 脚本引擎内存破坏漏洞（CNVD-2016-03020、CNVD-2016-03021、CNVD-2016-03120）、Microsoft Windows win32k 权限提升漏洞（CNVD-2016-03100、CNVD-2016-03103）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/webinfo/show/3847

2、 Adobe 产品安全漏洞

Adobe Acrobat DC 等都是美国奥多比（Adobe）公司的产品。Acrobat DC 是一套桌面版 PDF 解决方案；Acrobat Reader DC 是一套用于查看、打印和批注 PDF 的工具。Classic 和 Continuous 是 Acrobat DC 和 Acrobat Reader DC 产品下载中心所提供的两种更新机制。 本周，上述产品被披露存在任意命令执行、内存错误引用和内存破坏漏洞，攻击者可利用漏洞执行任意代码，控制受影响系统。

CNVD 收录的相关漏洞包括：多款 Adobe 产品内存破坏漏洞（CNVD-2016-03068、CNVD-2016-03069、CNVD-2016-03070、CNVD-2016-03071、CNVD-2016-03072、CNVD-2016-03073、CNVD-2016-03074、CNVD-2016-03075）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-2016-03068
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03069
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03070
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03071
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03072
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03073
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03074
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03075

3、 Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。 本周，上述产品被披露存在权限提升、任意代码执行、信息泄露和拒绝服务漏洞，攻击者可利用上述漏洞提升权限、执行任意代码、泄露敏感信息和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Android NVIDIA Video Driver 权限提升漏洞（CNVD-2016-02826、CNVD-2016-02827、CNVD-2016-02828、CNVD-2016-02829）、Android Mediaserver 提权漏洞（CNVD-2016-02845、CNVD-2016-02846、CNVD-2016-02847、CNVD-2016-02848）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-2016-02826
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02827
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02828
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02829
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02845
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02846
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02847
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02848

4、 PHP 产品安全漏洞

PHP 是 PHP Group 和开放源代码社区共同维护的一种开源的通用计算机脚本语言， PHP File Manager 是一套使用 PHP 脚本管理 Web 站点的应用程序。本周，上述产品被披露存在认证绕过、信息泄露和整数溢出漏洞，允许攻击者利用漏洞绕过密码访问、泄露敏感信息和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PHP 'exif_read_data()'函数信息泄露漏洞（CNVD-2016-02881、CNVD-2016-02882、CNVD-2016-02883）、PHP 信息泄露漏洞（CNVD-2016-

02884、CNVD-2016-02886）、PHP 存在未明漏洞（CNVD-2016-02887、CNVD-2016-02888 CNVD-2016-02885）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-2016-02881

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02882

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02883

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02884

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02885

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02886

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02887

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02888

5、 ASUS wireless routers 设计漏洞

wireless routers 是 ASUS 的路由器产品。本周，ASUS 被披露存在设计漏洞，允许攻击者利用漏洞够获得管理员 session。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-2016-02938

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-2016-02806	Cisco FirePOWER System Software 拒绝服务漏洞	高	Cisco 已经为此发布了一个安全公告（cisco-sa-20160504-firepower）以及相应补丁：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-firepower
CNVD-2016-02807	Cisco FirePOWER System Software 内核日志配置拒绝服务漏洞	高	Cisco 已经为此发布了一个安全公告（cisco-sa-20160504-fpkern）以及相应补丁:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-fpkern
CNVD-2016-02809	Trend Micro Email Encryption SQL 注入漏洞	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://esupport.trendmicro.com/solution/en-US/1114060.aspx
CNVD-2016-02858	IBM Java SDK 任意代码执行漏洞	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：http://www-01.ibm.com/support/docview.wss?uid=swg21982198

CNVD-2016-02865	ImageMagick Studio ImageMagick 任意文件读取漏洞	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.imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588
CNVD-2016-02872	Zabbix SIA Zabbix Agent 远程命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.zabbix.com/browse/ZBX-10741
CNVD-2016-02877	libpam-sshauth 本地提权漏洞	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.linux-pam.org/Linux-PAM-html/sag-pam_succeed_if.html
CNVD-2016-02874	Moxa MiiNePort 权限获取漏洞	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.moxa.com/
CNVD-2016-02893	HELP NetCommWireless HSPA 3G10WVE 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.netcommwireless.com/
CNVD-2016-02892	HELP NetCommWireless HSPA 3G10WVE 安全绕过漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.netcommwireless.com/

表 4 部分重要高危漏洞列表

小结：5 月 10 日，微软发布了 2016 年 5 月份的月度例行安全公告，共含 16 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Server、Office、Office Service、Web Apps、和.NET Framework 中存在的 36 个安全漏洞。其中，8 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码；此外，Adobe、Google、PHP 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限、泄露敏感信息和发起拒绝服务攻击等。另外，ASUS 被披露存在一个高危漏洞，允许攻击者利用漏洞获得管理员 session。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. WordPress 论坛插件 bbPress 存在存储型 XSS 漏洞

近日，WordPress 母公司 Automattic 发布了 bbPress 2.5.9 版本，在这个官方的 WordPress 论坛插件的最新版本中，修复了一个威胁程度较高的存储型 XSS 漏洞，攻击者可以利用漏洞于 Web 平台中植入恶意代码，而恶意代码会被存储于后台或数据库中，随后其他用户访问受影响页面时，便会执行攻击者此前植入的恶意代码，从而实现跨站的攻击。影响范围包括现有的 bbPress 版本，即版本< 2.5.9 的皆会受到影响。

参考链接：http://www.freebuf.com/vuls/103520.html

2. 微软 Office 365 平台 SAML 服务漏洞，可越权访问其他用户资源

近期，两位安全研究人员，Klemen Bratec 及 Ioannis Kakavas，公布了他们发现的一个在 Microsoft Office 365 平台上的 SAML 服务漏洞，攻击者可以利用这个漏洞突破访问权限限制，越权获取到受害用户的 Office 365 账户信息，并可借此访问他们的邮箱以及存储在 OneDrive（微软的云存储服务）上的文件等等。目前该漏洞已经被微软临时修复。

参考链接：http://www.freebuf.com/vuls/103718.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