国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 09 月 07 日-2015 年 09 月 13 日 **2015 年第 37 期**

本周漏洞基本情况

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 144 个，其中高危漏洞 65 个、中危漏洞 69 个、低危漏洞 10 个。上述漏洞中，可利用来实施远程攻击的漏洞有 129 个。本周收录的漏洞中，已有 137 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“Fortinet FortiClient 提权漏洞”、“Fortinet FortiClient 任意代码执行漏洞”零日漏洞，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 5 家成员单位、合作伙伴及个人报送了本周收录的全部 144 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、天融信、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、深圳市深信服电子科技有限公司及白帽子向 CNVD 提交了 454 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	130	130
安天实验室	126	0
天融信	92	0
绿盟科技	33	0
恒安嘉新	14	0
乌云	281	281

漏洞盒子	32	32
深圳市深信服电子科技有限公司	3	3
江西分中心	3	3
福建分中心	1	1
上海分中心	1	1
安徽分中心	1	1
个人	2	2
报送总计	719	454
录入总计	144（去重）	454

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Google、MediaWiki 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	24	17%
2	Google	15	10%
3	MediaWiki	12	8%
4	FFmpeg	9	6%
5	Cisco	6	4%
6	Basware	6	4%
7	Drupal	4	3%
8	EMC	4	3%
9	Fortinet	4	3%
10	其他	60	42%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 144 个漏洞。其中应用程序漏洞 104 个，Web 应用漏洞 32 个，网络设备漏洞 6 个，安全产品漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	104
Web 应用漏洞	32
网络设备漏洞	6
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

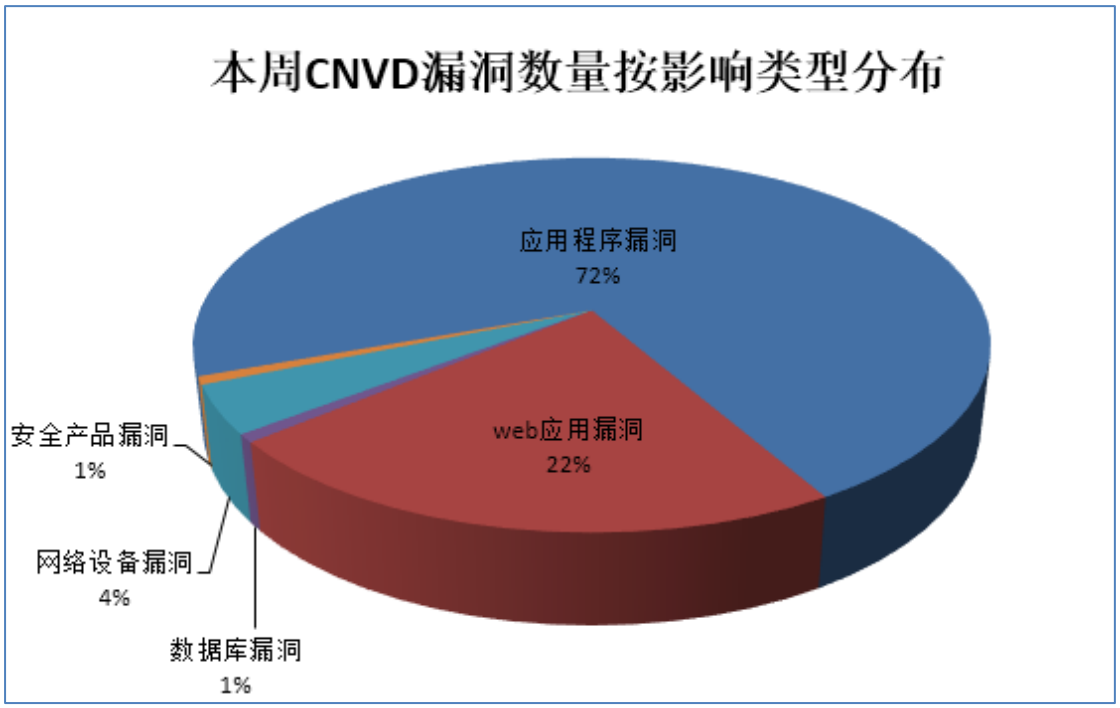

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 7 个电信行业漏洞、1 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下图表所示）。其中，“Moxa Industrial Managed Switch 权限提升漏洞、IBM WebSphere Commerce 敏感信息泄露漏洞、Advantech WebAccess 缓冲区溢出漏洞（CNVD-2015-05943）”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-05846	Moxa Industrial Managed Switch 跨站脚本漏洞	中	是
电信	CNVD-2015-05849	Moxa Industrial Managed Switch 拒绝服务漏洞	中	是
电信	CNVD-2015-05848	Moxa Industrial Managed Switch 权限提升漏洞	高	是
电信	CNVD-2015-05865	Cisco NX-OS ARP 服务重启漏洞	中	是

电信	CNVD-2015-05863	Cisco ASR 1000 Series Router 分片 IPv 4 处理拒绝服务漏洞	中	是
电信	CNVD-2015-05886	IBM WebSphere Commerce 敏感信息泄露漏洞	高	是
电信	CNVD-2015-05887	IBM WebSphere MQ MQI 呼叫目标通道代理崩溃漏洞	中	是
移动互联网	CNVD-2015-05811	Siemens COMPAS Mobile 应用程序输入验证漏洞	中	是
工控系统	CNVD-2015-05943	Advantech WebAccess 缓冲区溢出漏洞（CNVD-2015-05943）	高	是
工控系统	CNVD-2015-05939	Schneider Electric Modicon PLC 跨站脚本漏洞	低	是
工控系统	CNVD-2015-05940	Schneider Electric Modicon PLC 文件包含漏洞	低	是

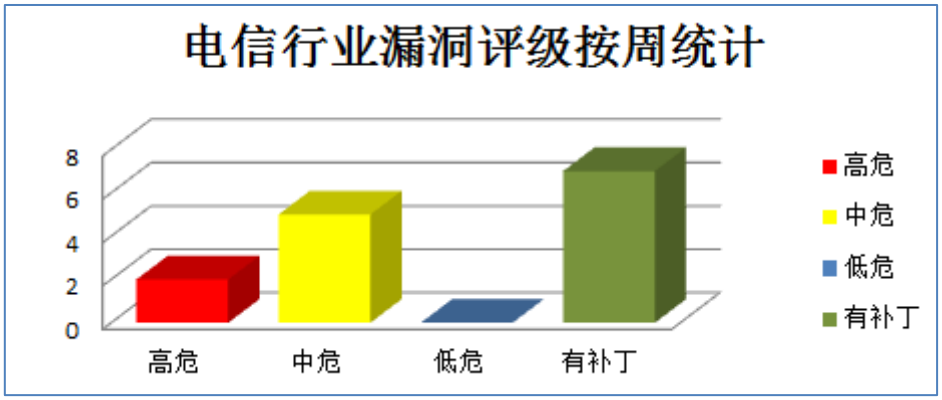

图 1 电信行业漏洞统计

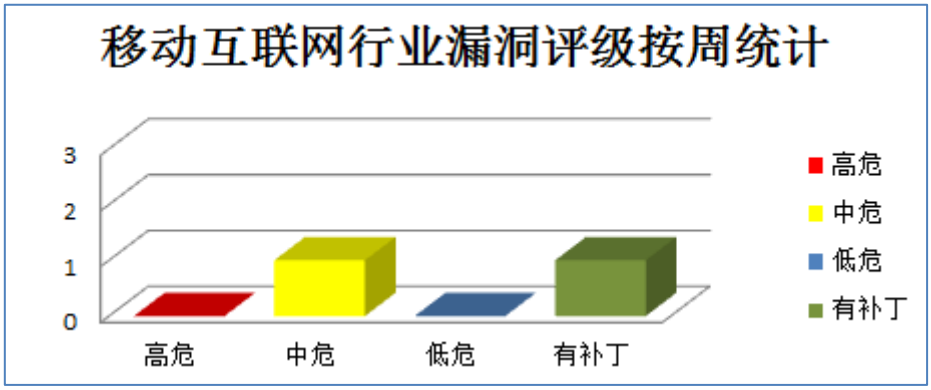

图 2 移动互联网行业漏洞统计

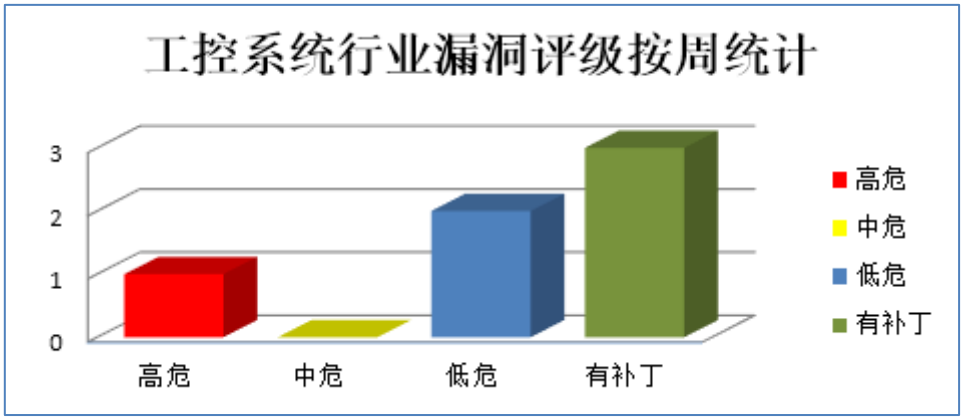

图 3 工控系统行业漏洞统计

本周重要漏洞信息

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

9 月 8 日，微软发布了 2015 年 9 月份的月度例行安全公告，共含 12 项更新，修复了 Microsoft Windows、Internet Explorer、Office、Edge、Lync、SharePoint Foundation、Exchange Server、Business Server、Lync Server 和.NET Framework 中存在的 56 个安全漏洞。其中，5 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，攻击者可以执行远程代码，提升权限，绕过安全功能限制，获得敏感信息，进行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-05906、CNVD-2015-05907、CNVD-2015-05908、CNVD-2015-05909、CNVD-2015-05910、CNVD-2015-05911、CNVD-2015-05912、CNVD-2015-05913）。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/3697

2、 Google 产品安全漏洞

Google Chrome 是一款基于 WEB 的浏览器。本周，上述产品被披露存在内存错误引用、限制绕过漏洞。攻击者利用漏洞绕过安全限制、执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 存在多个未明漏洞（CNVD-2015-05858）、Google Chrome Blink 内存错误引用漏洞（CNVD-2015-05856）、Google Chrome WebRequest API 访问限制绕过漏洞、Google Chrome Printing 内存错误引用漏洞、Google Chrome Skia 内存错误引用漏洞、Google Chrome Blink 同源策略绕过漏洞（CNVD-2015-05805）、Google Chrome OpenJPEG 内存错误引用漏洞、Google V8 存在未明漏

洞（CNVD-2015-05802）。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-2015-05858

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05856

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05854

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05852

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05851

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05805

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05801

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05802

3、FFmpeg 产品安全漏洞

FFmpeg 是 FFmpeg 团队的一套可录制、转换以及流化音视频的完整解决方案。本周，上述产品被披露存在拒绝服务漏洞。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：FFmpeg ff_mjpeg_decode_frame 拒绝服务漏洞、FFmpeg ff_sbr_apply 拒绝服务漏洞、FFmpeg ff_mpv_common_init 拒绝服务漏洞、FFmpeg destroy_buffers 拒绝服务漏洞、FFmpeg allocate_buffers 拒绝服务漏洞、FFmpeg sws_init_context 拒绝服务漏洞、FFmpeg ff_frame_thread_init 拒绝服务漏洞、FFmpeg ff_rv34_decode_init_thread_copy 拒绝服务漏洞。其中，除“FFmpeg ff_frame_thread_init 拒绝服务漏洞、FFmpeg ff_rv34_decode_init_thread_copy 拒绝服务漏洞”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-2015-05938

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05937

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05936

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05932

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05935

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05931

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05930

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05927

4、Basware 产品安全漏洞

Basware Banking（Maksuliikenne）是芬兰 Basware 公司的一套与银行建立连接对自己的金融进行管理的软件。本周，上述产品被披露存在信息泄露、信任管理、安全绕过和拒绝服务漏洞。攻击者可利用漏洞获得敏感信息、绕过安全限制和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Basware Banking 信任管理漏洞（CNVD-2015-05812、

CNVD-2015-05813）、Basware Banking 信息泄露漏洞（CNVD-2015-05816、CNVD-2015-05817）、Basware Banking 拒绝服务漏洞、Basware Banking 安全绕过漏洞。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-2015-05812

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05813

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05816

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05817

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05814

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05815

5、 Fortinet FortiClient 提权漏洞

Fortinet FortiClient 是美国飞塔（Fortinet）公司一套终端安全解决方案，为终端用户提供防病毒、加密等服务。本周，Fortinet FortiClient 被披露存在综合评级为“高危”的提权漏洞。攻击者利用该漏洞可获得权限提升。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-2015-05797

更多高危漏洞如表 3 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-2015-05806	HP Intelligent Provisioning 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这个安全问题，请到厂商的主页下载：https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04756070
CNVD-2015-05810	Ricoh DL FTP Server 缓冲区溢出漏洞	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：http://www.ricohpmmc.com/
CNVD-2015-05847	Symantec Ghost 越界索引远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=secu
CNVD-2015-05862	PCS pcsd web UI 操作系统命令注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：http://rhn.redhat.com/errata/RHSA-2015-1700.html

CNVD-2015-05883	IPPUSBXD 权限提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：http://www.ubuntu.com/usn/USN-2725-1
CNVD-2015-05884	PowerDNS Authoritative Server 报文处理目标服务崩溃漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：https://doc.powerdns.com/md/security/powerdns-advisory-2015-02/
CNVD-2015-05895	BIND OpenPGP 密钥处理拒绝服务漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：https://kb.isc.org/article/AA-01291/74/CVE-2015-5986%3A-An-incorrect-boundary-check-can-trigger-a-REQUIRE-assertion-failure-in-openpgpkey_61.c.html
CNVD-2015-05893	BIND DNSSEC Key 处理错误拒绝服务漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：https://kb.isc.org/article/AA-01287/74/CVE-2015-5722%3A-Parsing-malformed-keys-may-cause-BIND-to-exit-due-to-a-failed-assertion-in-buffer.c.html
CNVD-2015-05891	Chicken 存在未明缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://code.call-cc.org/releases/4.10.0/NEWS
CNVD-2015-05944	HP UCMDB 本地信息泄露漏洞	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://softwaresupport.hp.com/group/softwaresupport/search-result/

表 3 部分高危漏洞列表

小结：9 月 8 日，微软发布了 2015 年 9 月份的月度例行安全公告，共含 12 项更新，修复了 Microsoft Windows、Internet Explorer、Office、Edge、Lync、SharePoint Foundation、Exchange Server、Business Server、Lync Server 和.NET Framework 中存在的 56 个安全漏洞。此外，Google、FFmpeg、Basware 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、绕过安全限制、执行任意代码或发起拒绝服务攻击。另外，Fortinet FortiClient 被披露存在一个高危零日漏洞，攻击者利用该漏洞可获得权限提升。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Symantec 修补 Ghost Explorer Utility 产品漏洞

Symantec Ghost Explorer Utility 是 GHO 文件浏览工具。

本周，Symantec 修补了上述产品存在的远程代码执行漏洞，避免攻击者利用漏洞执行任意代码。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/63691

本周要闻速递

1. 安全研究员曝光 FireEye 核心产品 0day 漏洞

FireEye 是一家为企业提供安全防护产品的美国网络安全公司。近日，研究人员 Kristian Erik Hermansen 从 FireEye 核心产品中发现一个 0day 漏洞，会导致未经授权的文件泄露。

参考链接：http://www.freebuf.com/news/77543.html

2. PayPal 修复存储型 XSS 漏洞

PayPal 是国外著名 B2C 网站 eBay 的子公司。研究者发现 PayPal 电子支付服务中含有存储型 XSS 漏洞，攻击者可以上传特殊文件对注册用户进行攻击。这个漏洞能够被用于上传恶意文件，从而进行大规模的攻击。目前 PayPal 已经及时发布了补丁来修复此漏洞。

参考链接：http://www.freebuf.com/news/77252.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