

信息安全漏洞周报

2014 年 6 月 9 日-2014 年 6 月 15 日

2014 年第 24 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 159 个，其中高危漏洞 77 个、中危漏洞 72 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 141 个。本周收录的漏洞中，已有 149 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。本周互联网上出现“Videos Tube 存在多个 SQL 注入漏洞”的零日攻击代码，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 6 家成员单位、及个人报送了本周收录的全部 159 个漏洞。报送情况如表 1 所示。其中，安天实验室、天融信、启明星辰、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心及多个白帽子向 CNVD 提交了 11 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	162	0
天融信	152	0
启明星辰	140	0
绿盟科技	47	0
奇虎 360	26	26
恒安嘉新	1	0
CNCERT 山西分中心	6	6
CNCERT 新疆分中心	1	1
个人	4	4

报送总计	539	37
录入总计	159（去重）	37

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、ownCloud、SAP 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	62	39%
2	ownCloud	11	7%
3	SAP	9	6%
4	Cisco	6	4%
5	IBM	6	4%
6	Adobe	6	4%
7	Google	4	3%
8	EMC	4	3%
9	Red Hat	3	2%
10	其他	48	28%

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 159 个漏洞。其中应用程序漏洞 128 个，操作系统漏洞 11 个，WEB 应用漏洞 10 个，网络设备漏洞 9 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	128
操作系统漏洞	11
WEB 应用漏洞	10
网络设备漏洞	9
安全产品漏洞	1

表 3 漏洞按影响类型统计表

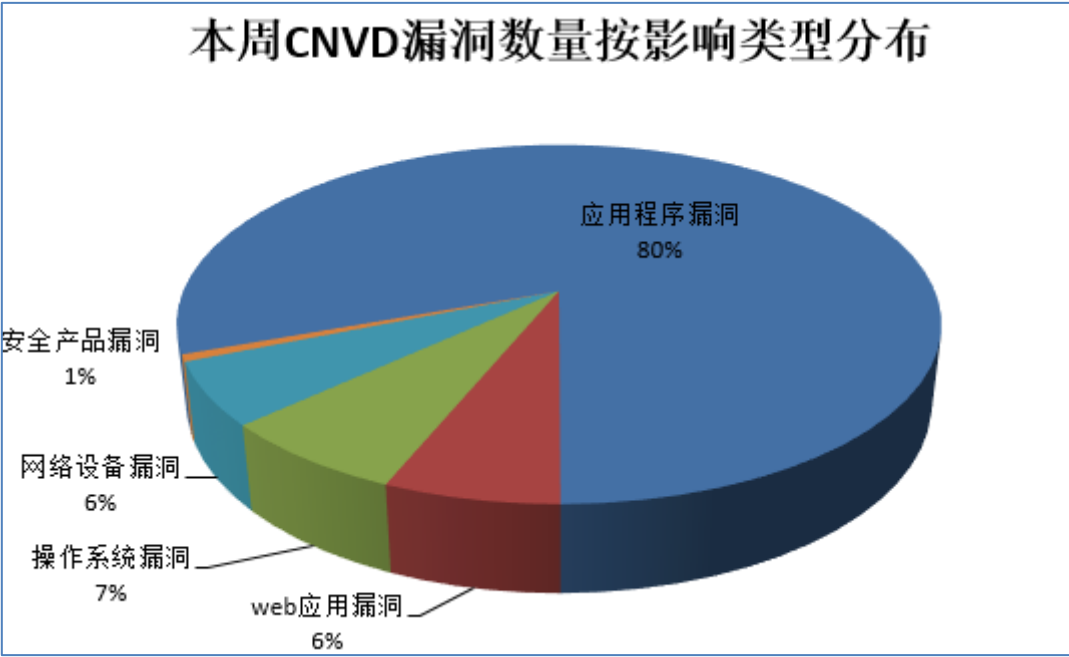


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 4 个电信行业漏洞和 3 个工控行业漏洞（如下图表所示）。其中，“多款 D-Link 产品缓冲区溢出漏洞、多个 CCOPA-DATA Zenon 产品拒绝服务漏洞”的综合评级均为“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-2014-03524	Cisco WebEx Meeting Server 用户枚举漏洞	中	否
电信	CNVD-2014-03523	Cisco Wireless LAN Controller 拒绝服务漏（CNVD-2014-03523）	中	是
电信	CNVD-2014-03544	多款 D-Link 产品缓冲区溢出漏洞	高	是
电信	CNVD-2014-03603	Cisco Unified Communications Manager 存在多个任意文件访问漏洞	中	是
工控系统	CNVD-2014-03522	Triangle MicroWorks SCADA Data Gateway TLS/DTLS 信息泄露漏洞	中	是
工控系统	CNVD-2014-03596	多个 COPA-DATA Zenon 产品本地拒绝服务漏洞	中	是
工控系统	CNVD-2014-03595	多个 CCOPA-DATA Zenon 产品拒绝服务漏洞	高	是

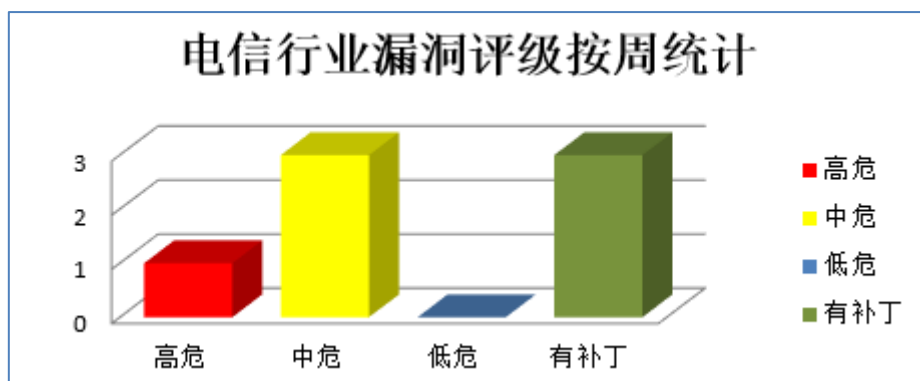


图 2 电信行业漏洞统计

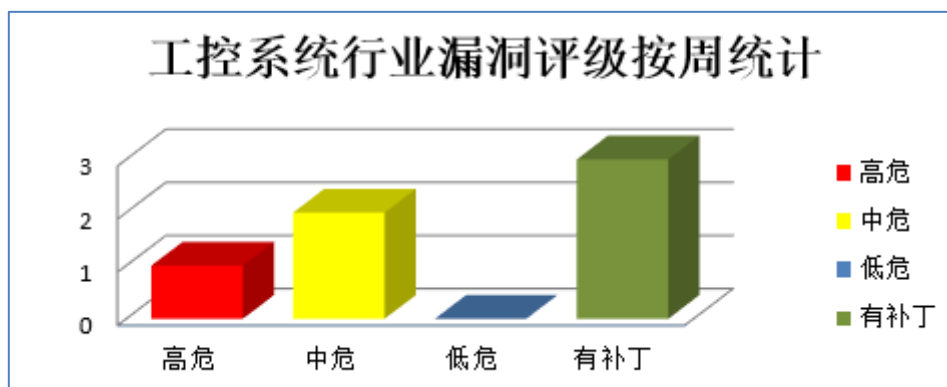


图 3 工控行业漏洞统计

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

6 月 11 日，微软发布了 2014 年 6 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、Office、Internet Explorer、和 Lync Server 中存在的 66 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以攻击者可以执行任意代码，获得敏感信息，进行拒绝服务攻击。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-03546、CNVD-2014-03547、CNVD-2014-03548、CNVD-2014-03549、CNVD-2014-03550）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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/3454>

2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序; Adobe Air 是一款 Adobe 公司出品的跨操作系统的运行时库。本周, 上述产品被披露存在多个安全漏洞, 攻击者可利用漏洞构建恶意文件, 诱使用户解析, 进行未授权操作或执行任意代码。

CNVD 收录的相关漏洞包括: Adobe Flash Player/AIR 存在未明安全绕过漏洞 (CNVD-2014-03633、CNVD-2014-03634)、Adobe Flash Player/AIR 存在未明内存破坏漏洞 (CNVD-2014-03632)、Adobe Flash Player/AIR 存在未明跨站脚本漏洞 (CNVD-2014-03635、CNVD-2014-03636)。其中, 除 “Adobe Flash Player/AIR 存在未明跨站脚本漏洞 (CNVD-2014-03635、CNVD-2014-03636)” 外, 其余漏洞的综合评级均为 “高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新, 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-2014-03633>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03634>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03632>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03635>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03636>

3、EMC 产品安全漏洞

EMC Documentum 是一款企业文档和图像管理工具。EMC RSA Adaptive Authentication 是美国易安信 (EMC) 公司的一套基于风险的全面身份认证和欺诈检测平台。本周, 上述产品被披露存在多个安全漏洞, 攻击者可利用漏洞提升权限、执行未授权操作或注入任意 Web 脚本和 HTML 代码。

CNVD 收录的相关漏洞包括: EMC Documentum Content Server 远程特权提升漏洞、EMC Documentum Content Server Shell 命令注入漏洞、EMC Documentum Content Server 远程特权升级漏洞、EMC RSA Adaptive Authentication 跨站脚本漏洞。其中, 除 “EMC RSA Adaptive Authentication 跨站脚本漏洞” 外, 其余漏洞的综合评级均为 “高危”。厂商已经发布了上述漏洞的修补程序。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-2014-03586>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03528>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03529>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03519>

4、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周, 上述产品被披露存在多个安全漏洞, 攻击者可利用漏洞使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括: Google Chrome Media 处理堆溢出漏洞、Google Chrome 文件系统 API 内存错误引用漏洞、Google Chrome SPDY 重入处理越界读漏洞、G

oogle Chrome 剪贴板缓冲区溢出漏洞。其中,“Google Chrome Media 处理堆溢出漏洞、Google Chrome 文件系统 API 内存错误引用漏洞”的综合评级为“高危”。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-2014-03629>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03631>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03609>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03630>

5、Videos Tube 存在多个 SQL 注入漏洞

Videos Tube 是一套视频软件。本周, Videos Tube 产品被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者利用漏洞可通过 url 参数到 videocatphp 或 singlephp 执行任意 SQL 命令。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-2014-03509>

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-2014-03505	ownCloud Server 权限访问漏洞	高	请安装厂商已发布的最新版本或补丁: http://owncloud.org/about/security/advisories/oc-sa-2014-011/
CNVD-2014-03511	ATEN IP KVM Switch 存在未明拒绝服务漏洞	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.aten.com/IP-KVM.htm
CNVD-2014-03534	openstack-foreman-installer 安全绕过漏洞	高	请安装厂商已发布的最新版本或补丁: http://www.redhat.com/
CNVD-2014-03533	Red Hat openstack-neutron package-7 权限提升漏洞	高	请安装厂商已发布的最新版本或补丁: https://access.redhat.com/home
CNVD-2014-03532	Samsung iPOLiS Device Manager ActiveX Control 存在多个远程代码执行漏洞	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.samsungsecurity.com/support/online_tool.asp
CNVD-2014-03531	Samsung iPOLiS Device Manager 'FindConfigChildeKeyList()'方法栈缓冲区溢出漏洞	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://update.websamsung.net/Tools/iPOLiS%20Device%20Manager/iPOLiS%20Device%20Manager_v1.8.7_setup_Full.zip
CNVD-2014-03544	多款 D-Link 产品缓冲区溢出漏洞	高	请安装厂商已发布的最新版本或补丁： http://www.dlink.com/
CNVD-2014-03542	dpkg-dev 目录遍历漏洞	高	请安装厂商已发布的最新版本或补丁： https://www.debian.org/distrib/packages
CNVD-2014-03600	Xen 本地权限提升漏洞	高	请安装厂商已发布的最新版本或补丁： http://xenbits.xen.org/xsa/advisory-98.html
CNVD-2014-03595	多个 CCOPA-DATA Zenon 产品拒绝服务漏洞	高	请安装厂商已发布的最新版本或补丁： http://www.copadata.com/en/support.html

表 3 部分高危漏洞列表

小结：本周，微软发布了 2014 年 6 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、Office、Internet Explorer、和 Lync Server 中存在的 66 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。此外，Adobe、EMC、Google 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行未经授权操作、注入任意脚本代码、提升权限或者发起拒绝服务攻击。Videos Tube 产品被披露存在一个高危零日漏洞。攻击者利用漏洞可通过 url 参数到 videocatphp 或 singlephp 执行任意 SQL 命令。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、Linux 修补 Kernel 产品漏洞

Linux Kernel 是一款开源的操作系统。

本周，Linux 修补了上述产品存在的拒绝服务漏洞，避免攻击者可利用漏洞使内核崩溃，发起拒绝服务攻击。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/46392>

<http://www.cnvd.org.cn/patchInfo/show/46393>

本周要闻速递

1. 微软发布大量安全补丁

北京时间 6 月 11 日凌晨，微软发布了新一轮软件安全补丁，本次发布的安全补丁数量很大，仅 IE 浏览器的补丁就高达 59 个，这之中还包括其在 5 月 22 日公开的一个关键漏洞。总结所有的更新，微软此次发布了七款安全补丁，共覆盖 66 个不同安全漏洞。补丁主要用来修复 Win7、Win8 等系统和 IE、Office 等软件，之前已“停止服务”的 Windows XP 则没有得到补丁。

参考链接：<http://www.cet.com.cn/itpd/yw/1219164.shtml>

2. iOS7 再曝锁屏漏洞

有用户发现了 iOS 7 系统最新的锁屏安全漏洞，利用该漏洞可以绕过默认密码输入界面。这次的安全漏洞最快允许攻击者 5 秒钟完成。当然，这已经不是 iOS 7 第一次被爆出有安全漏洞。这次的安全漏洞需要一些特定的条件才能正常工作。需要注意的是，通过该方法绕过锁屏后，只能访问锁屏前正在前台运行的应用。虽然，不能访问整个 iOS 7 系统，但根据不同的应用，用户的隐私还是有危险的。经过测试后发现，iOS 7.0.6 和 iOS 7.1.1 系统均受到影响。想要测试该漏洞，通知中心需要有一个未接来电，而且需要可以在锁屏界面访问控制中心。

参考链接：<http://article.pchome.net/content-1728766-all.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