

信息安全漏洞周报

2014 年 6 月 2 日-2014 年 6 月 8 日

2014 年第 23 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**低**。

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 100 个，其中高危漏洞 22 个、中危漏洞 62 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 86 个。本周收录的漏洞中，已有 72 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“Trend Micro InterScan Messaging Security Virtual Appliance 跨站脚本漏洞”、“PHP-Nuke 'Submit_News'组件 SQL 注入漏洞”等零日攻击代码，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 100 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、绿盟等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及多个白帽子向 CNVD 提交了 31 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	117	0
安天实验室	105	0
启明星辰	70	0
奇虎 360	39	0
绿盟科技	34	0
恒安嘉新	33	0
习科网络安全	16	16
CNCERT 山西分中心	9	9
CNCERT 黑龙江分中心	1	1

个人	5	5
报送总计	429	31
录入总计	100（去重）	31

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、WordPress、Drupal 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	IBM	5	5%
2	WordPress	5	5%
3	Drupal	5	5%
4	OpenSSL	4	4%
5	TYPO3	4	4%
6	Microsoft	3	3%
7	Linux	2	2%
8	Red Hat	2	2%
9	Hua Wei	2	2%
10	其他	68	68%

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 100 个漏洞。其中应用程序漏洞 67 个，WEB 应用漏洞 26 个，网络设备漏洞 2 个，操作系统漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	67
WEB 应用漏洞	26
网络设备漏洞	2
数据库漏洞	0
操作系统漏洞	5
安全产品漏洞	0

表 3 漏洞按影响类型统计表

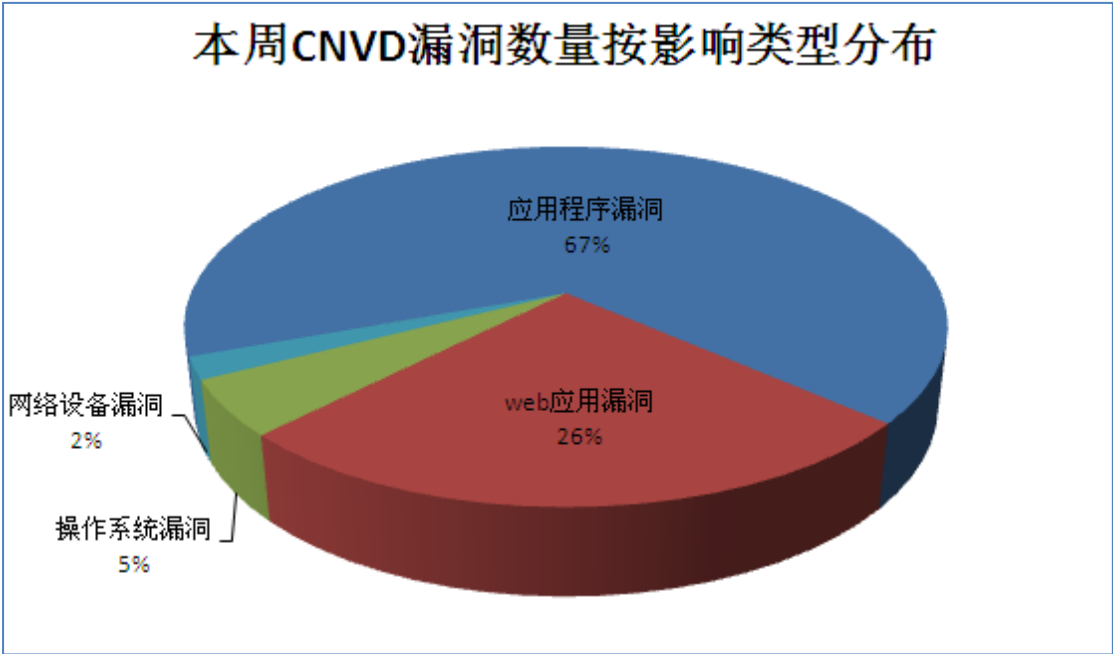


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 5 个电信行业漏洞和 5 个工控行业漏洞（如下列表所示）。其中，“Huawei Campus 系列路由器存在多个远程堆缓冲区溢出漏洞、Cogent Real-Time Systems DataHub 目录遍历漏洞、Cogent Real-Time Systems DataHub 反射型跨站脚本漏洞”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-2014-03429	Apache Tomcat 'java/org/apache/tomcat/util/buf/Ascii.java'整数溢出漏洞	中	是
电信	CNVD-2014-03428	IBM WebSphere Service Registry and Repository 跨站脚本漏洞	中	是
电信	CNVD-2014-03465	Huawei E303 路由器跨站请求伪造漏洞	中	否
电信	CNVD-2014-03494	IBM Tivoli Identity Manager 和 Security Identity Manager 跨站请求伪造漏洞	低	是
电信	CNVD-2014-03495	Huawei Campus 系列路由器存在多个远程堆缓冲区溢出漏洞	高	是
工控系统	CNVD-2014-03392	Cogent Real-Time Systems DataHub 不安全密码哈希漏洞	中	是
工控系统	CNVD-2014-03266	Cogent Real-Time Systems DataHub 目录遍历漏洞	高	是
工控系统	CNVD-2014-03277	Cogent Real-Time Systems DataHub 反射型跨站脚本漏洞	高	是
工控系统	CNVD-2014-03278	SCADA Data Gateway 串口链接设备本	低	是

		地拒绝服务漏洞		
工控系统	CNVD-2014-03282	SCADA Data Gateway IP 链接设备远程拒绝服务漏洞	中	是

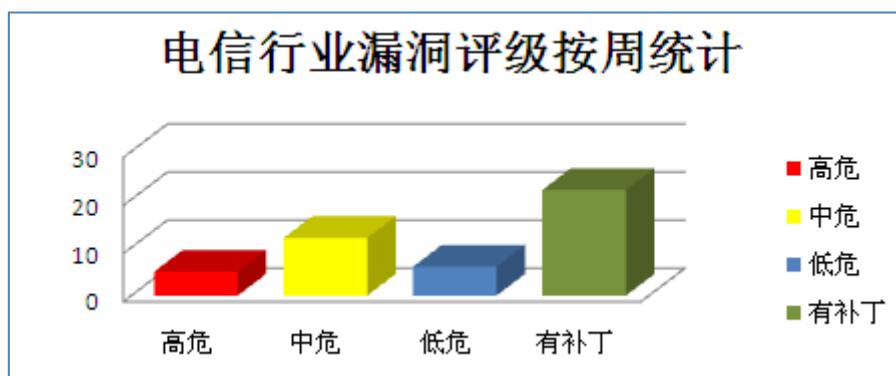


图 1 电信行业漏洞统计

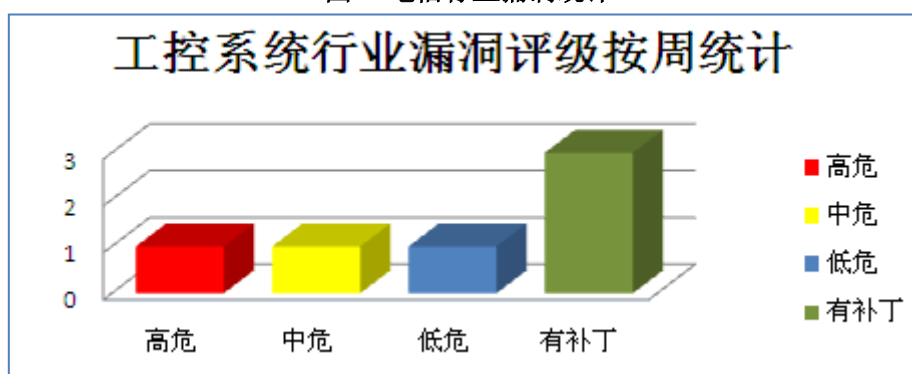


图 3 工控行业漏洞统计

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、IBM 产品安全漏洞

IBM Tivoli Identity Manager，简称 TIM，是 IBM 身份的生命周期的管理工具；IBM Connections 是企业级社交软件，实现文档管理和协作办公功能；IBM API Management 是一套完整的解决方案来帮助企业安全地创建、管理和连接应用程序接口(API)，以便将其产品和服务拓展至各种移动渠道；IBM Sterling Control Center 是美国 IBM 公司的一套文件传输控制和管理工具。该工具提供文件传输环境的统一视图、环境异常响应等功能；IBM WebSphere Service Registry and Repository (WSRR) 是美国 IBM 公司的一个用于服务交互端点描述的主元数据存储库，它提供了存储、访问和管理有关服务信息的功能，并且是 SOA 实现的关键组成部分。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、执行未授权操作或者注入任意脚本代码。

CNVD 收录的相关漏洞包括：IBM Tivoli Identity Manager 和 Security Identity Manager 跨站请求伪造漏洞、IBM Connections 用户关注跨站请求伪造漏洞、IBM API Management Topology 存在未明信息泄露漏洞、IBM Sterling Control Center 开放重定向漏洞、IBM WebSphere Service Registry and Repository 跨站脚本漏洞。除“IBM API Management Topology 存在未明信息泄露漏洞”外，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-2014-03494>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03478>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03477>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03436>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03428>

2、Drupal 产品安全漏洞

Drupal 是使用 PHP 语言编写的开源内容管理框架，它由内容管理系统和 PHP 开发框架共同构成；AddressField Tokens 是其中的一个通过添加令牌支持扩展 addressfield（地址字段定义模块）的模块；Google Authenticator 是其中的一个扩展模块，该模块是美国谷歌（google）公司开发的一款身份验证器。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作或注入任意脚本代码。

CNVD 收录的相关漏洞包括：Drupal AddressField Tokens 模块跨站脚本漏洞、Drupal Webserver Auth 模块安全绕过漏洞、Drupal Realname Registration 模块安全绕过漏洞、Drupal Node Access Keys 模块访问绕过漏洞、Drupal Google Authenticator 登录模块访问绕过漏洞。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-2014-03431>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03469>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03470>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03418>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03404>

3、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款 WEB 浏览器；Microsoft Windows 是一款流行的操作系统。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、使应用程序崩溃或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 'TryGetValueAndRemove()'方法拒绝服务漏洞、Microsoft Windows Touch Injection API 本地拒绝服务漏洞、Microsoft Windows 'GreSetPaletteEntries()'本地拒绝服务漏洞。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-2014-03413>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03408>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03407>

4、OpenSSL 产品安全漏洞

OpenSSL 是一个安全套接字层密码库,囊括主要的密码算法、常用的密钥和证书封装管理功能及 SSL 协议,并提供丰富的应用程序供测试或其它目的使用。本周,OpenSSL 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、发起拒绝服务或以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括: OpenSSL 中间人安全绕过漏洞、OpenSSL DTLS 远程拒绝服务漏洞、OpenSSL 拒绝服务漏洞、OpenSSL 内存破坏漏洞。其中“OpenSSL 内存破坏漏洞”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-2014-03493>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03491>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03490>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03489>

5、TYPO3 安全漏洞

TYPO3 是一款开源的内容管理系统。本周,该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、注入任意脚本代码。

CNVD 收录的相关漏洞包括: TYPO3 HTTP Host Header 欺骗漏洞、TYPO3 Extbase Framework 信息泄露漏洞、TYPO3 后端组件存在多个跨站脚本漏洞、TYPO3 Grid Elements 存在未明跨站脚本漏洞。其中,除“TYPO3 Extbase Framework 信息泄露漏洞”外,厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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-2014-03492>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03476>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03459>

6、Xilisoft Video Converter Ultimate 'quserex.dll' DLL 加载任意代码执行漏洞

Xilisoft Video Converter Ultimate 是一款视频转换应用。本周,Video Converter Ultimate 产品被披露存在综合评级为“高危”的'quserex.dll' DLL 加载任意代码执行漏洞。攻击者利用漏洞可构建恶意文件,诱使用户加载,并以应用程序上下文执行恶意代码。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-2014-03438>

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-2014-03406	GnuTLS 'gnutls_handshake.c'内存破坏漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.gnutls.org/security.html#GNUTLS-SA-2014-3
CNVD-2014-03416	NICE Recording eXpress 存在多个漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.nice.com/compliance-call-recording
CNVD-2014-03424	SolarWinds Network Configuration Manager 'PEstrarg1'缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.zerodayinitiative.com/advisories/ZDI-14-133/
CNVD-2014-03423	webEdition CMS 'setup.php'远程命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.webedition.org/de/aktuelles/webedition-cms/
CNVD-2014-03422	webEdition CMS 'we_fs.php' 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： http://www.webedition.org/de/aktuelles/webedition-cms/
CNVD-2014-03430	CoSoSys Endpoint Protector SQL注入漏洞	高	暂无
CNVD-2014-03445	Cogent Real-Time Systems DataHub 目录遍历漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://cogentdatahub.com/Download_Software.html
CNVD-2014-03443	DCMTK 本地特权提升漏洞	高	暂无
CNVD-2014-03440	Ericom AccessNow Server 栈缓冲区溢出远程代码执行漏洞	高	暂无
CNVD-2014-03449	Rocket Servergraph 'userRequest' servlet 请求远程命令注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM、Drupal、Microsoft、TYPO3 多款产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息、执行未授权操作、注入任意脚本代码或者发起拒绝服务攻击。 OpenSSL 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，发起拒绝服务或以应用程序上下文执行任意代码。此外，Video Converter Ultimate 产品被披露存在一个高危零日漏洞，攻击者可利用漏洞构建恶意文件，诱使用户加载，并以应

用程序上下文执行恶意代码。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、WordPress 修补 2 个插件漏洞

WordPress 是一种使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网志，Contextual Related Posts 是其中的一个用于显示相关文章的插件，可自动通过算法匹配文章的上下文；Query Interface Plugin 是客户同组件的交互接口插件。

本周，WordPress 修补了上述 2 个插件存在的 SQL 注入漏洞，避免攻击者利用漏洞获取敏感信息或者执行任意 SQL 指令。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://42.96.134.153/patchInfo/show/46150>

<http://42.96.134.153/patchInfo/show/46092>

本周要闻速递

1. OpenSSL 严重 CCS 注入安全漏洞

OpenSSL 的 ChangeCipherSpec (CCS) 处理近日曝出严重安全漏洞，该漏洞使得攻击者可以拦截恶意中间节点，进行加密和解密数据，同时强迫使用弱密钥的 SSL 客户端暴露在恶意节点中。一旦软件使用到 OpenSSL 的受影响版本，通过网页浏览、电子邮件和 VPN 进行内容和身份验证等加密通讯时就会有被篡改的风险。

参考链接：<http://soft.yesky.com/security/133/37562133.shtml>

2. 加密协议库 GnuTLS 再现漏洞

近日再现安全通讯库 GnuTLS 重大漏洞，该漏洞可能使黑客执行远程恶意代码。这已经是 GnuTLS 今年第二起安全漏洞事件。上周五 Codenomicon 安全人员 Joonas Kuori lehto 首先通报 GnuTLS 漏洞，并很快由 Red Hat 安全研发人员 Nikos Mavrogiannopoulos 发布修补程式，以修补受影响的 GnuTLS 3.3.3、GnuTLS 3.2.15 及 GnuTLS 3.1.25。此后，GnuTLS 开发人员又发布更新版 GnuTLS 3.3.4，以修补另一项与安全无关的瑕疵。

参考链接：<http://soft.yesky.com/security/47/37561047.shtml>

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