国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 06 月 22 日-2015 年 06 月 28 日 **2015 年第 26 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 143 个，其中高危漏洞 39 个、中危漏洞 96 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 125 个。本周收录的漏洞中，已有 103 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“WordPress Aviary Image Editor Add-on For Gravity Forms 插件任意文件上传漏洞”、“libmimedir 特制文件任意代码执行漏洞”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、合作伙伴及个人报送了本周收录的全部 143 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、广州白狐网络科技有限公司、四川大学信息安全研究所、乌云、漏洞盒子及白帽子向 CNVD 提交了 604 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	373	373
安天实验室	272	0
启明星辰	149	0
天融信	84	0
恒安嘉新	67	0

绿盟科技	29	0
乌云	198	198
漏洞盒子	17	17
广州白狐网络科技有限公司	3	3
四川大学信息安全研究所	1	1
CNCERT 上海分中心	3	3
CNCERT 福建分中心	3	3
CNCERT 江西分中心	2	2
个人	4	4
报送总计	1205	604
录入总计	143（去重）	604

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、PHP、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	Cisco	17	12%
2	PHP	12	8%
3	Drupal	7	5%
4	Hospira	7	5%
5	ABRT	7	5%
6	WordPress	7	5%
7	w1.fi	6	4%
8	Linux	3	2%
9	Symantec	3	2%
10	其他	74	52%

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 143 个漏洞。其中应用程序漏洞 88 个，WEB 应用漏洞 27 个，网络设备漏洞 18 个，安全产品漏洞 5 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	88
WEB 应用漏洞	27
网络设备漏洞	18
安全产品漏洞	5
操作系统漏洞	5

表 3 漏洞按影响类型统计表

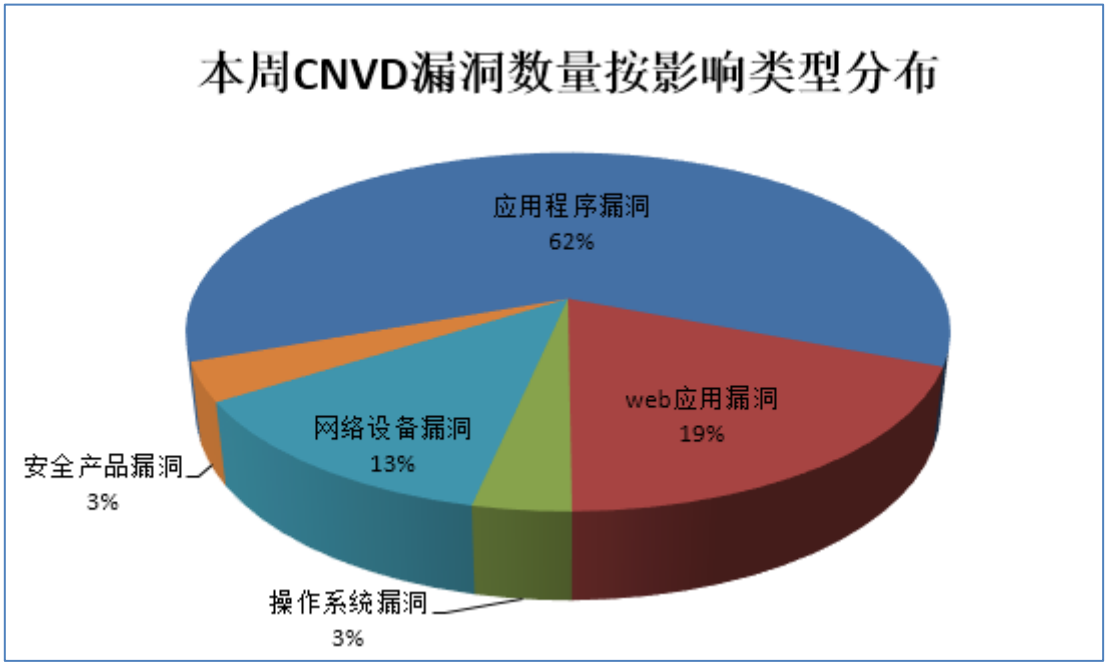

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞， 2 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图表所示）。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-03916	Alcatel-Lucent CellPipe 7130 路由器跨站脚本漏洞	中	否
电信	CNVD-2015-03949	Cisco IOS XR IPv6 ipv6_io 服务处理拒绝服务漏洞	中	是

电信	CNVD-2015-03953	Samsung Galaxy S 手机远程代码执行漏洞	中	否
电信	CNVD-2015-03955	Cisco IOS XR SSH 链接终止拒绝服务漏洞	中	是
电信	CNVD-2015-03981	Cisco ASR 9000 IOS XR 资源管理错误漏洞	中	是
电信	CNVD-2015-03986	Wireshark GSM DTAP 解析器远程拒绝服务漏洞	中	是
电信	CNVD-2015-03987	Cisco uBR10000 Series Universal Broadband Routers 信息泄露漏洞	中	是
电信	CNVD-2015-03988	Cisco ASR 5000 Series Router GGSN TCP/IP 处理拒绝服务漏洞	中	是
电信	CNVD-2015-03989	Cisco NX-OS LLDP 处理拒绝服务漏洞	中	是
电信	CNVD-2015-03992	Airties RT-210 多个参数跨站脚本漏洞	中	否
电信	CNVD-2015-04005	Cisco IOS Software UBR Devices SNMP 子系统拒绝服务漏洞	中	是
电信	CNVD-2015-04004	Cisco Wireless LAN Controller IPv6 数据包处理拒绝服务漏洞	中	是
电信	CNVD-2015-03995	Cisco Secure Access Control System 和 Cisco Identity Services Engine 信息泄露漏洞	中	是
电信	CNVD-2015-04020	多款 Samsung Galaxy 设备中间人攻击漏洞	中	是
电信	CNVD-2015-04019	多款 Samsung Galaxy 设备目录遍历漏洞	中	是
移动互联网	CNVD-2015-04020	多款 Samsung Galaxy 设备中间人攻击漏洞	中	是
移动互联网	CNVD-2015-04019	多款 Samsung Galaxy 设备目录遍历漏洞	中	是
工控系统	CNVD-2015-03907	Wind River VXWorks TCP 可预测漏洞	中	是

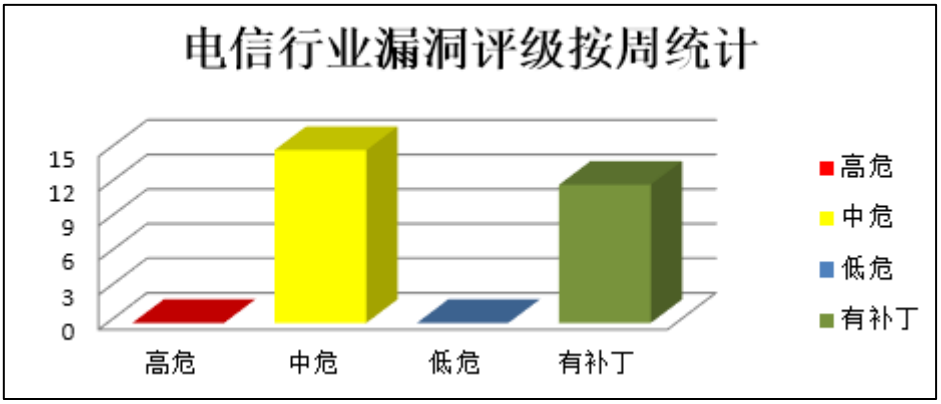

图 1 电信行业漏洞统计

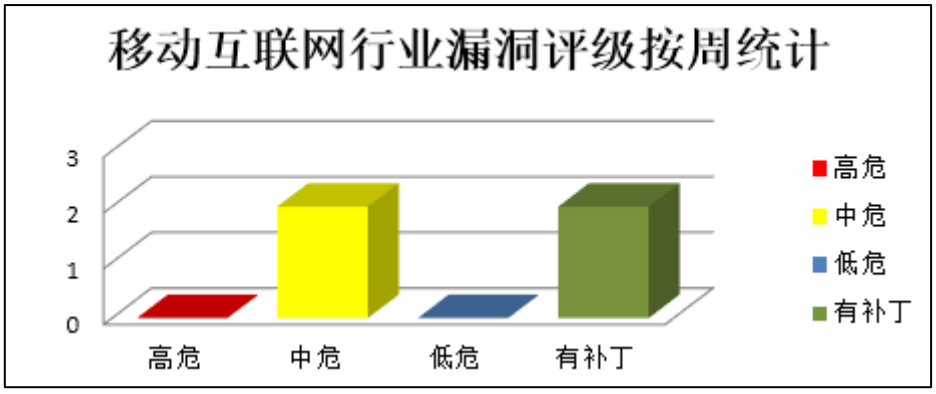

图 2 移动互联网行业漏洞统计

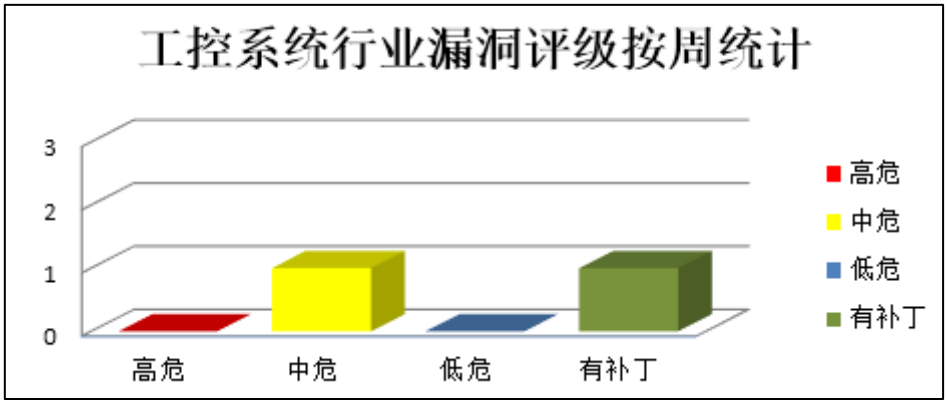

图 3 工控系统行业漏洞统计

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、 Cisco 产品安全漏洞

Cisco Unified MeetingPlace 是美国思科（Cisco）公司的一套多媒体会议解决方案。该解决方案提供了将语音、视频和 Web 会议集成在一起的用户环境。Cisco Jabber 是美国思科（Cisco）公司的一套跨设备协作系统。该系统提供语音、视频、桌面共享和会议等功能。Cisco WebEx Meetings Server 是一款思科公司推出的思科会议中心实现。Cisco Data Center Analytics Framework（DCAF）是美国思科（Cisco）公司的一套数据中心分析框架。Cisco Web Security Appliance（WSA）是美国思科（Cisco）公司的一套 Web 安全设备。Cisco FireSIGHT System Software 是美国思科（Cisco）公司的一套管理中心软件，它支持集中管理采用 FirePOWER Services 的 Cisco ASA 和思科 FirePOWER 网络安全设备的网络安全和运行功能的软件。本周，上述产品被披露存在信息泄露、跨站请求伪造和跨站脚本漏洞。攻击者可利用漏洞获取敏感信息、执行未授权操作、或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Cisco Unified MeetingPlace 信息泄露漏洞（CNVD-2015-03993）、Cisco Jabber 信息泄露漏洞、Cisco WebEx Meeting Center 跨站脚本漏洞、Cisco WebEx Meeting Center 信息泄露漏洞、Cisco Data Center Analytics Framework 跨站请求伪造漏洞、Cisco WebEx Meeting Center 合法用户名泄露漏洞、Cisco Web Security Appliance 跨站脚本漏洞（CNVD-2015-03921）、Cisco FireSIGHT System Software 跨站脚本漏洞（CNVD-2015-03926）。目前，除“Cisco Web Security Appliance 跨站脚本漏洞（CNVD-2015-03921）、Cisco FireSIGHT System Software 跨站脚本漏洞（CNVD-2015-03926）、Cisco Data Center Analytics Framework 跨站请求伪造漏洞”外，厂商已经发布了其余漏洞的修补程序。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-2015-03993
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03994
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03979
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03980
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03982
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03954
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03921
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03926

2、 PHP 产品安全漏洞

PHP 是一款通用脚本语言。本周，该产品被披露存在内存破坏、拒绝服务和限制绕过漏洞。攻击者可利用漏洞获取敏感信息、绕过安全限制或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PHP 'incomplete_class.c'内存破坏漏洞、PHP libmagick 'libmagic/softmagic.c'拒绝服务漏洞（CNVD-2015-03966、CNVD-2015-03965）、PHP SOAP 访问存在多个内存破坏漏洞、PHP SOAP 访问远程内存破坏漏洞、PHP 空指针间接引用拒绝服务漏洞、PHP 空指针引用限制绕过漏洞、PHP DOM 及 GD 扩展限制绕过漏洞。其中，“PHP 'incomplete_class.c'内存破坏漏洞、PHP SOAP 访问存在多个内存破坏漏洞、PHP SOAP 访问远程内存破坏漏洞”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-2015-03970
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03966
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03965
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03968
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03969
http://www.cnvd.org.cn/flaw/show/CNVD-2015-03911

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03963

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03967

3、Drupal 产品安全漏洞

Drupal 是 Drupal 社区所维护的一套用 PHP 语言开发的免费、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得敏感信息、劫持会话、重定向页面或进行跨站攻击。

CNVD 收录的相关漏洞包括：Drupal jQuery Update 模块开放重定向漏洞、Drupal Field UI 模块开放重定向漏洞、Drupal Overlay 模块开放重定向漏洞、Drupal OpenID 模块会话劫持漏洞、Drupal Render 缓存系统信息泄露漏洞、Drupal Apache Solr Real-Time 模块访问绕过漏洞、Drupal Petition 模块跨站脚本漏洞（CNVD-2015-03892）。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-2015-04036

http://www.cnvd.org.cn/flaw/show/CNVD-2015-04017

http://www.cnvd.org.cn/flaw/show/CNVD-2015-04034

http://www.cnvd.org.cn/flaw/show/CNVD-2015-04035

http://www.cnvd.org.cn/flaw/show/CNVD-2015-04018

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03959

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03892

4、Symantec 产品安全漏洞

Symantec Endpoint Protection 是一款为增强企业病毒防护与高级威胁防御能力而开发的防护软件。本周，该产品被披露存在 SQL 注入、拒绝服务和任意代码执行漏洞。攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Symantec Endpoint Protection 'sysplant.sys'拒绝服务漏洞、Symantec Endpoint Protection 管理控制台 SQL 注入漏洞、Symantec Endpoint Protection DLL 加载任意代码执行漏洞。其中“Symantec Endpoint Protection 管理控制台 SQL 注入漏洞”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-2015-03946

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03947

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03948

5、Eproductsurf 存在多个 SQL 注入漏洞

Eproductsurf 是阿联酋 Eproductsurf 公司的一套网站设计、网站开发和网络营销解决方案。本周，Eproductsurf 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者利

用该漏洞可控制应用程序，访问或修改数据库数据。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-2015-03997

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-2015-03900	CGI RESCUE BloBee 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.rescue.ne.jp/cgi/blobee/
CNVD-2015-03908	QEMU 'pit_ioport_read()'函数内存破坏漏洞	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://fabrice.bellard.free.fr/qemu/
CNVD-2015-03906	DedeCMS 任意代码执行漏洞	高	暂无
CNVD-2015-03909	Microsoft Internet Explorer ShowSaveFileDialog DLL 加载任意代码执行漏洞	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：http://www.microsoft.com/windows/ie/default.asp
CNVD-2015-03918	Milw0rm Clone Script SQL 注入漏洞	高	暂无
CNVD-2015-03917	Joomla! EQ Event Calendar 组件 SQL 注入漏洞	高	暂无
CNVD-2015-03939	Cacti‘get_hash_graph_template’函数 SQL 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://bugs.cacti.net/view.php?id=2572
CNVD-2015-03938	Cacti SQL 注入漏洞（CNVD-2015-03938）	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.cacti.net/release_notes_0_8_8d.php
CNVD-2015-03941	PCRE 'pcre_compile2()'函数堆缓冲区溢出漏洞	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.pcre.org/
CNVD-2015-03942	PCRE 'compile_branch()'函数堆缓冲区溢出漏洞	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.pcre.org/

表 3 部分高危漏洞列表

小结：本周，Cisco 产品被披露存在信息泄露、跨站请求伪造和跨站脚本漏洞。攻击者可利用漏洞获取敏感信息、执行未授权操作、或进行跨站脚本攻击。此外，PHP、Drupal、Symantec 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敏感信息、绕过安全限制、重定向页面、劫持会话、执行任意代码、进行跨站攻击或发起拒绝服务攻击。另外，Eproductsurf 被披露存在一个高危零日漏洞，攻击者利用该漏洞可控制应用程序，访问或修改数据库数据。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、Microsoft 修补 Internet Explorer 漏洞

Microsoft Internet Explorer 是微软公司推出的一款网页浏览器。

本周，Microsoft 修补了上述产品存在的任意代码执行漏洞，避免攻击者利用漏洞在当前用户上下文中执行任意代码。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/59859

本周要闻速递

1. 大量思科安全设备被曝存在默认 SSH 密钥

思科公司的安全专家发现，很多思科安全设备中存在一个默认 SSH 密钥，攻击者可以利用它们建立 SSH 连接，并能够控制设备。SSH 密钥的滥用反映了一个严重问题，即相关企业和机构都可能暴露在网络攻击风险之中。根据思科公司的消息，Web 安全虚拟设备、电子邮件安全虚拟设备和内容安全管理虚拟设备都受安全问题的影响。

参考链接：http://www.freebuf.com/news/71160.html

2. Ubuntu 曝本地权限提升漏洞（CVE-2015-1328），影响多个版本

由于特定情况下创建文件时的权限检查 bug，Ubuntu 操作系统曝本地权限提升漏洞，允许本地攻击者利用这个安全漏洞，可获取目标计算机最高权限。影响 Ubuntu 12.04、14.04、14.10、15.04 版本。目前 Ubuntu 官方已经修复了该漏洞。

参考链接：http://www.freebuf.com/news/70615.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