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 15 日-2015 年 06 月 21 日 **2015 年第 25 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 110 个，其中高危漏洞 28 个、中危漏洞 73 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 100 个。本周收录的漏洞中，已有 97 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“Spectris N-Tron 702-W Industrial Wireless Access Point 设备密钥漏洞”等零日漏洞，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 7 家成员单位、合作伙伴及个人报送了本周收录的全部 110 个漏洞。报送情况如表 1 所示。其中，奇虎、天融信、启明星辰、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research Lab、乌云、漏洞盒子及白帽子向 CNVD 提交了 530 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	288	288
天融信	153	3
启明星辰	80	0
安天实验室	44	0
绿盟科技	20	0
恒安嘉新	9	0

东软	3	0
乌云	208	208
漏洞盒子	19	19
High-Tech Bridge Security Research Lab	2	2
CNCERT 安徽分中心	2	2
CNCERT 福建分中心	1	1
个人	7	7
报送总计	836	530
录入总计	110（去重）	530

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、Adobe、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	16	15%
2	Adobe	10	9%
3	Drupal	8	7%
4	TYPO3	8	7%
5	WordPress	7	6%
6	VMware	7	6%
7	Igreks Inc.	7	6%
8	OpenSSL	5	5%
9	ZOHO	4	4%
10	其他	38	35%

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 110 个漏洞。其中应用程序漏洞 68 个，WEB 应用漏洞 26 个，网络设备漏洞 12 个，安全产品漏洞 3 个，操作系统漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	68
WEB 应用漏洞	26
网络设备漏洞	12
安全产品漏洞	3
操作系统漏洞	1

表 3 漏洞按影响类型统计表

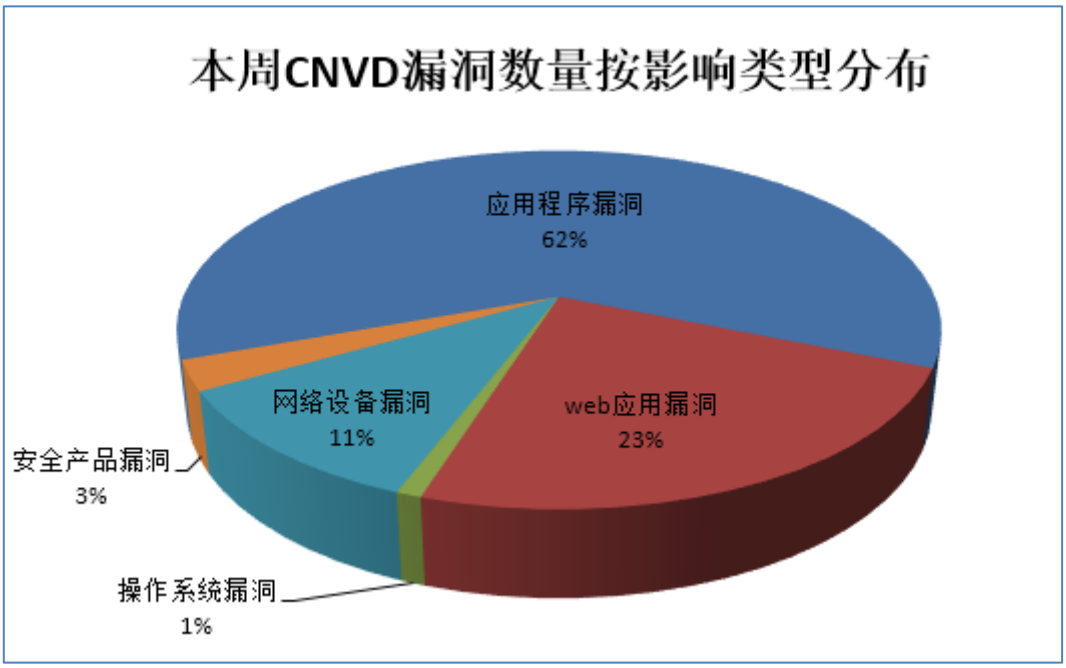

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞，1 个工控系统行业漏洞（如下图表所示）。其中，“RLE Nova-Wind Turbine HMI 不安全凭证漏洞”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-2015-03785	Alcatel OmniSwitch WEB 接口跨站请求伪造漏洞	低	否
电信	CNVD-2015-03783	Cisco Prime 网络控制系统特权提升漏洞	中	是
电信	CNVD-2015-03780	Cisco Catalyst 6500 Series Switches 拒绝服务漏洞	中	否

电信	CNVD-2015-03854	Cisco IOS XR Software 拒绝服务漏洞（CNVD-2015-03854）	中	是
电信	CNVD-2015-03843	Cisco Prime Collaboration Manager SQL 注入漏洞	中	是
电信	CNVD-2015-03886	Cisco Nexus 和 MDS NX-OS 拒绝服务漏洞	中	是
工控系统	CNVD-2015-03884	RLE Nova-Wind Turbine HMI 不安全凭证漏洞	高	是

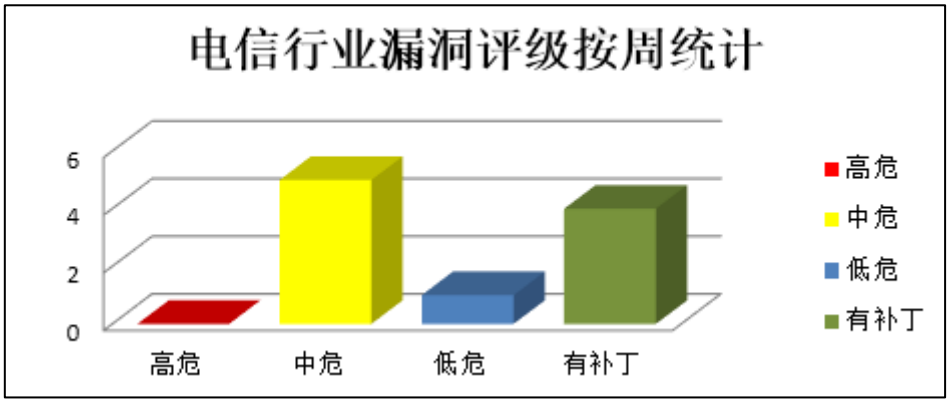

图 1 电信行业漏洞统计

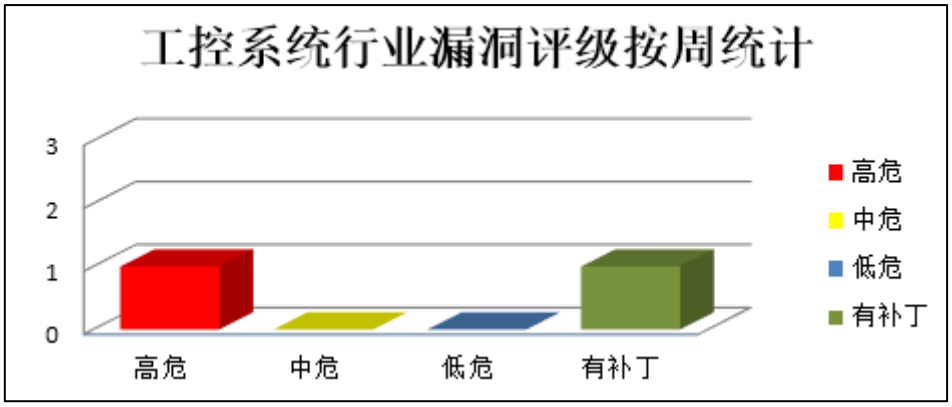

图 2 工控系统行业漏洞统计

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、 TYPO3 产品安全漏洞

TYPO3 是一套免费开源的内容管理系统。本周，该产品被披露存在 SQL 注入、任意文件上传和跨站脚本漏洞。攻击者可利用漏洞获取敏感信息、上传任意文件或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：TYPO3 Developer Log 扩展 SQL 注入漏洞、TYPO3 Frontend User Upload 任意文件上传漏洞、TYPO3 Job Fair 任意文件上传漏洞、TYPO

3 Store Locator 扩展 SQL 注入漏洞、TYPO3 wt_directory 扩展 SQL 注入漏洞、TYPO3 FAQ - Frequently Asked Questions 扩展 SQL 注入漏洞、TYPO3 Smoelenboek 扩展 SQL 注入漏洞、TYPO3 BE User Log 扩展跨站脚本漏洞。其中，除“TYPO3 BE User Log 扩展跨站脚本漏洞”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-2015-03853

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03851

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03852

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03848

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03849

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03847

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03846

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03850

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在信息泄露、安全绕过、权限提升和任意代码执行漏洞。攻击者可利用漏洞获取敏感信息、绕过安全限制、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 同源策略绕过信息泄露漏洞（CNVD-2015-03801）、Adobe Flash Player Flash broker for Internet Explorer 权限提升漏洞、Adobe Flash Player ASLR 安全保护绕过漏洞、Adobe Flash Player 栈溢出任意代码执行漏洞（CNVD-2015-03802）、Adobe Flash Player 整数溢出任意代码执行漏洞、Adobe Flash Player 内存错误引用任意代码执行漏洞（CNVD-2015-03796、CNVD-2015-03797、CNVD-2015-03798）。其中，除“Adobe Flash Player 同源策略绕过信息泄露漏洞（CNVD-2015-03801）、Adobe Flash Player Flash broker for Internet Explorer 权限提升漏洞、Adobe Flash Player ASLR 安全保护绕过漏洞”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-2015-03801

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03799

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03800

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03802

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03803

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03796

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03797

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03798

3、OpenSSL 产品安全漏洞

OpenSSL 是一种开放源码的 SSL 实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。本周，该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：OpenSSL do_free_upto 函数拒绝服务漏洞、OpenSSL dtls1_clear_queues 函数拒绝服务漏洞、OpenSSL X509_cmp_time 函数拒绝服务漏洞、OpenSSL PKCS7_dataDecode 函数拒绝服务漏洞、OpenSSL BN_GF2m_mod_inv 函数拒绝服务漏洞。其中，“OpenSSL dtls1_clear_queues 函数拒绝服务漏洞”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-2015-03813

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03812

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03810

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03811

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03809

4、VMware 安全漏洞

VMware 是桌面到数据中心虚拟化解决方案的厂商。本周，该产品被披露存在内存分配错误、拒绝服务和任意代码执行漏洞。攻击者可利用漏洞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：VMware Workstation/Player/Fusion 特制 RPC 命令拒绝服务漏洞、VMware Horizon Client for windows 任意代码执行漏洞（CNVD-2015-03816、CNVD-2015-03817）、VMware Workstation/Player/Fusion 'TPView.ddl'拒绝服务漏洞、VMware Workstation/Player/Fusion 'TPInt.dll'拒绝服务漏洞、VMware Workstation/Player/Fusion 'TPInt.dll'任意代码执行漏洞、VMware Horizon Client for windows 内存分配错误漏洞。其中“VMware Workstation/Player/Fusion 特制 RPC 命令拒绝服务漏洞”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-2015-03815

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03816

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03817

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03824

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03822

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03818

http://www.cnvd.org.cn/flaw/show/CNVD-2015-03823

5、Spectris N-Tron 702-W Industrial Wireless Access Point 设备密钥漏洞

Spectris N-Tron 702-W Industrial Wireless Access Point devices 是一款无线接入点设备。本周，Spectris N-Tron 702-W Industrial Wireless Access Point devices 被披露存在综合评级为“高危”的设备密钥漏洞。攻击者利用该漏洞可通过已知的密钥获取敏感信息，或未授权访问。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-2015-03889

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-2015-03789	ZOHO NetFlow Analyzer 身份验证绕过漏洞	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://support.zoho.com/portal/manageengine/helpcenter/articles/vulnerability-fix-for-fails-to-restrict-access-permissions-cross-site-scripting-cross-site-request-forgery-over-build-10250
CNVD-2015-03819	Tidy ‘tmbstr.c’堆缓冲区溢出漏洞	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://tidy.sourceforge.net/
CNVD-2015-03820	Xen QEMU PCNET 控制器堆溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://xenbits.xen.org/xsa/advisory-135.html
CNVD-2015-03837	ISPConfig 'monitor/show_sys_state.php' 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://bugtracker.ispconfig.org/index.php?do=details&task_id=3898
CNVD-2015-03840	Bonita BPM 路径遍历漏洞	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://community.bonitasoft.com/blog/bonita-bpm-653-available
CNVD-2015-03838	ISPConfig '/admin/users_edit.php' 跨站请求伪造漏洞	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://bugtracker.ispconfig.org/index.php?do=details&task_id=3898
CNVD-2015-03855	Vesta Control Panel OS 命令注入漏洞	高	Vesta Control Panel 0.9.8-14 已修复此漏洞，建议用户下载使用：http://vestacp.com

CNVD-2015-03884	RLE Nova-Wind Turbine HMI 不安全凭证漏洞	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.rle.international/de/
CNVD-2015-03878	Igreks MilkyStep Light 和 Professional SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请用户及时下载更新：http://milkystep.com
CNVD-2015-03883	Igreks MilkyStep OS 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://milkystep.com/

表 3 部分高危漏洞列表

小结：本周，TYPO3 产品被披露存在 SQL 注入、任意文件上传和跨站脚本漏洞。攻击者可利用漏洞获取敏感信息、上传任意文件或进行跨站脚本攻击。此外，Adobe、OpenSSL、VMware 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、提升权限、执行任意代码或发起拒绝服务攻击。另外，Spectris N-Tron 702-W Industrial Wireless Access Point devices 被披露存在一个高危零日漏洞，攻击者利用该漏洞可通过已知的密钥获取敏感信息，或未授权访问。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、McAfee 修补 ePolicy Orchestrator 漏洞

McAfee ePolicy Orchestrator 是一种业界领先的系统安全管理解决方案，能够帮助企业有效抵御各种恶意威胁和攻击。

本周，McAfee 修补了上述产品存在的跨站脚本漏洞，避免攻击者利用漏洞注入任意 Web 脚本或 HTML。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/59755

本周要闻速递

1. SAP HANA 系统曝安全漏洞，静态密钥存在数据库里

SAP 知名内存数据库管理系统 HANA 被曝存在安全漏洞，其静态加密密钥居然存放在数据库中。ERPScan 的研究人员在阿姆斯特丹举行的黑帽大会上展示了这个漏洞。ERPScan 的首席技术官 Alexander Polyakov 称，攻击者可以有多种方法进行攻击：诸如

SQL 注入来窃取 SAP 数据库中的密钥、使用目录遍历，或者 XXE 注入攻击(XML External Entity attack,XML 外部实体注入攻击)。默认的加密密钥被用来保护平台里的数据，包括密码和平台备份。另一方面，由于 SAP 的管理员们很少会更改默认的加密密钥，这也使得平台容易受到攻击。

参考链接：http://www.freebuf.com/news/70535.html

2. 全球风力发电和太阳能系统存安全缺陷，攻击者可干预能源供给

德国安全研究员 Maxim Rupp 在清洁能源系统（太阳能和风力发电系统）上发现了多个安全问题，攻击者可能会利用此漏洞干扰能源的供给。其受影响的系统有：

XZERES 442SR WindTurbine；

Sinapsi eSolar Light；

RLE Nova-Wind Turbine；

参考链接：http://www.freebuf.com/news/70020.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