国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 02 月 29 日-2016 年 03 月 06 日　　2016 年第 10 期

本周漏洞态势研判情况

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 102 个，其中高危漏洞 30 个、中危漏洞 67 个、低危漏洞 5 个。漏洞平均分值为 5.76 分。本周收录的漏洞中，涉及 0day 漏洞 14 个（占 14%）。其中互联网上出现“ManageEngine Firewall Analyzer 'runQuery.do' SQL 注入漏洞”、“ProjectSend 存在多个漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。此外，本周收录涉及党政机关企事事件型漏洞总数 1945 个，与上周（690 个）环比增长 182%。

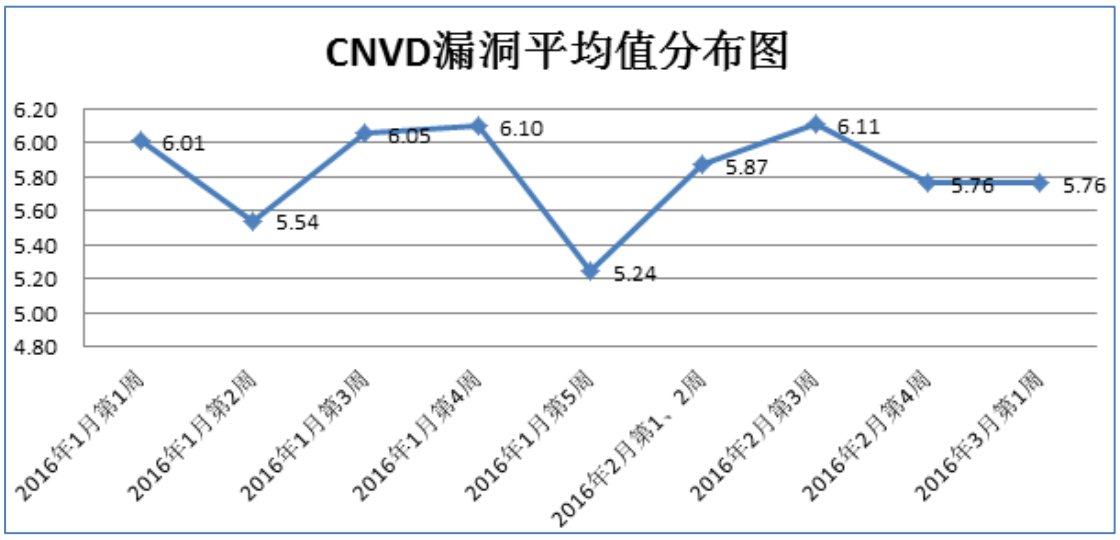

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

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 102 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、天融信、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子、广州白狐网络科技有限公司及白帽子向 CNVD

提交了 1945 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(补天平台)	1296	1296
安天实验室	106	0
天融信	51	0
恒安嘉新	22	0
H3C	5	0
知道创宇	2	1
绿盟科技	1	0
乌云	579	579
漏洞盒子	25	25
广州白狐网络科技有限公司	1	1
CNCERT 宁夏分中心	4	4
CNCERT 陕西分中心	2	2
CNCERT 福建分中心	1	1
个人	36	36
报送总计	2131	1945
录入总计	102（去重）	1945

表 1 成员单位上报漏洞统计表

注：本周与 360 公司补天平台接口出现回补情况，统计数量出现激增。

本周漏洞按类型和厂商统计

本周，CNVD 收录了 102 个漏洞。其中应用程序漏洞 75 个，Web 应用漏洞 13 个，操作系统漏洞 7 个，网络设备漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	75
Web 应用漏洞	13

操作系统漏洞	7
网络设备漏洞	7

表 2 漏洞按影响类型统计表

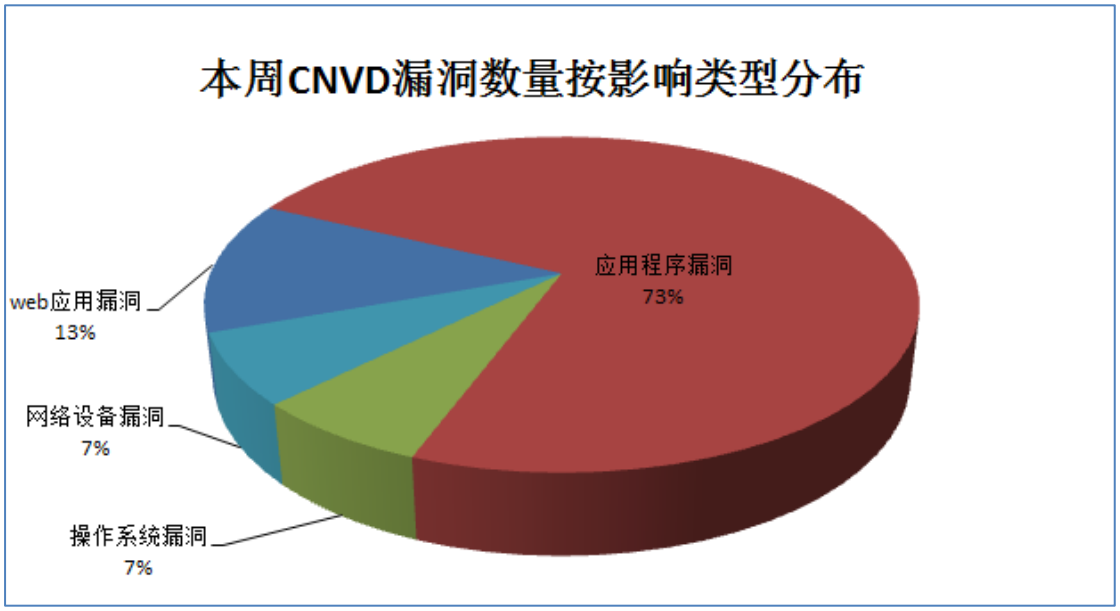

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Wireshark、IBM、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Wireshark	12	12%
2	IBM	10	10%
3	Cisco	7	7%
4	OpenSSL	6	6%
5	Yeager	6	6%
6	Squid	5	5%
7	CloudBees	5	5%
8	phpMyAdmin	4	4%
9	QNAP	4	4%
10	其他	43	41%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞、3 个工控系统行业漏洞（如下图所示）。

其中，“Cisco Nexus 9000 Application Centric Infrastructure Mode 拒绝服务漏洞、Cisco Application Policy Infrastructure Controller 和 Nexus 9000 ACI Mode Switches 安全绕过漏洞”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，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

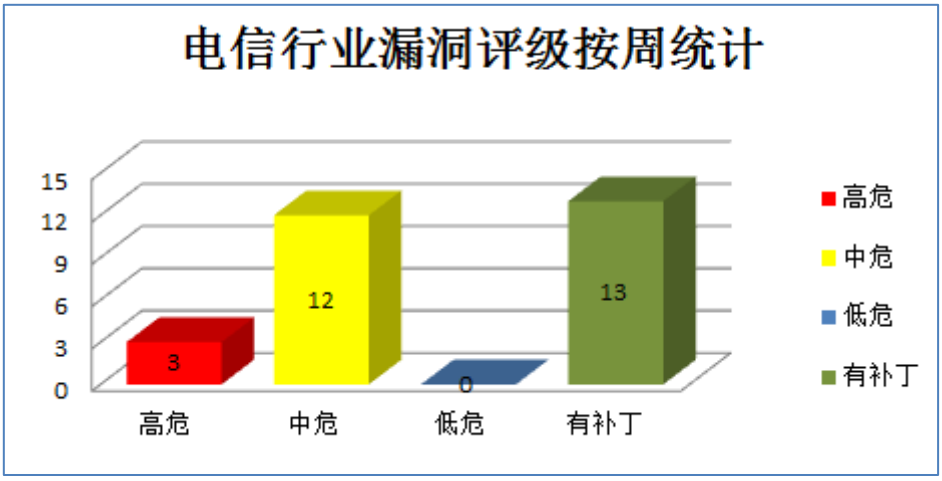

图 3 电信行业漏洞统计

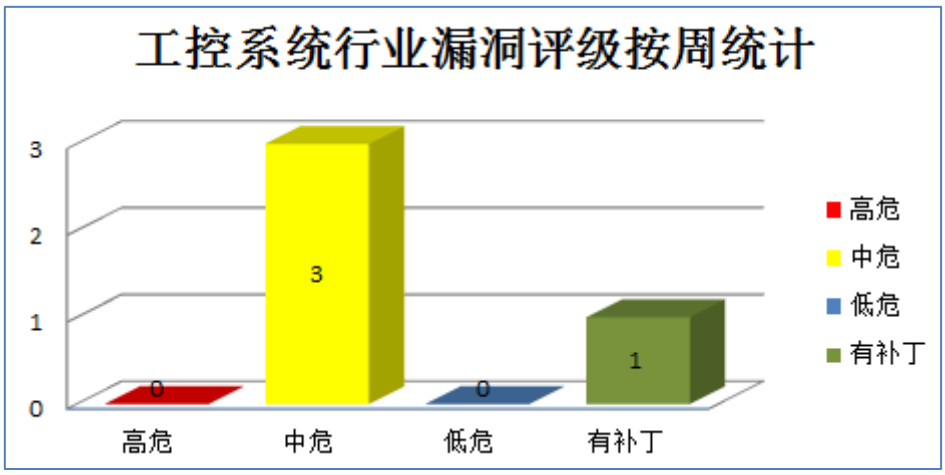

图 4 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 OpenSSL 产品安全漏洞

OpenSSL 是 OpenSSL 团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈

希算法、安全散列算法等。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可进行跨协议攻击和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：OpenSSL 模幂运算旁路攻击漏洞、OpenSSL SRP_VBASE_get_by_user 内存泄露漏洞、OpenSSL DSA 代码双重释放漏洞、OpenSSL Bleichenbacher oracle 漏洞、OpenSSL SSLv2 分治型会话密钥恢复漏洞、OpenSSL 跨协议攻击漏洞。其中，“OpenSSL 跨协议攻击漏洞”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-2016-01456

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01438

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01437

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01436

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01435

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01367

2、 IBM 产品安全漏洞

IBM WebSphere Portal 是美国 IBM 公司的一套企业门户软件。该软件能够创建一个联接企业内部和外部的平台，可让员工、客户和供应商等通过该平台访问企业内部数据。本周，上述产品被披露存在跨站脚本、开放重定向、拒绝服务漏洞等，攻击者利用漏洞可注入任意 Web 脚本或 HTML、重定用户到任意 web 网站或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal XML 解析器拒绝服务漏洞、IBM WebSphere Portal 跨站脚本漏洞（CNVD-2016-01422、CNVD-2016-01424、CNVD-2016-01420、CNVD-2016-01419）、IBM WebSphere Portal 设计漏洞、IBM WebSphere Portal 开放重定向漏洞（CNVD-2016-01416）。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-2016-01423

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01422

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01424

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01420

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01419

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01418

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01416

3、 Wireshark 产品安全漏洞

Wireshark 是最流行的网络协议解析器。本周，上述产品被披露存在拒绝服务漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Wireshark 拒绝服务漏洞（CNVD-2016-01446、CNV

D-2016-01445、CNVD-2016-01444、CNVD-2016-01448、CNVD-2016-01447、CNVD-2016-01449）、Wireshark DNP3 解析器拒绝服务漏洞、Wireshark HiQnet 解析器拒绝服务漏洞。其中，“Wireshark DNP3 解析器拒绝服务漏洞”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-2016-01446

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01445

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01444

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01448

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01447

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01449

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01408

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01407

4、 Yeager 产品安全漏洞

Yeager 是一套开源的内容管理系统。本周，该产品被披露存在 SQL 注入、跨站脚本、跨站请求伪造和任意文件上传漏洞，攻击者利用漏洞可获得数据库敏感信息、进行跨站脚本和跨站请求伪造攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Yeager 跨站请求伪造漏洞、Yeager SQL 注入漏洞、Yeager SQL 注入漏洞（CNVD-2016-01401、CNVD-2016-01400）、Yeager 跨站脚本漏洞、Yeager 任意文件上传漏洞。其中，除“Yeager 跨站请求伪造漏洞、Yeager 跨站脚本漏洞”外，其余漏洞的综合评级均为“高危”。目前，厂商已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-2016-01403

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01402

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01401

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01400

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01405

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01404

5、 ManageEngine Firewall Analyzer 'runQuery.do' SQL 注入漏洞

ZOHO ManageEngine Firewall Analyzer 是美国卓豪（ZOHO）公司的一套基于 Web 的防火墙日志分析工具，它能收集、关联分析和汇报整个企业范围内的防火墙、proxy 伺服器和 Radius 伺服器上的日志。本周，ZOHO ManageEngine Firewall Analyzer 被披露存在 SQL 注入漏洞，攻击者可利用漏洞控制应用程序，访问或修改数据库数据。目前，厂商尚未发布漏洞修补程序。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-2016-01340

更多高危漏洞如表 4 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-2016-01342	Ubuntu Linux 本地权限提升漏洞（CNVD-2016-01342）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.ubuntu.com/
CNVD-2016-01345	Ubuntu Linux 本地权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.ubuntu.com/
CNVD-2016-01371	JoyentSmartOS 存在多个漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://smartos.org/
CNVD-2016-01373	sos 不安全文件权限漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/sosreport/sos
CNVD-2016-01375	CloudBees Jenkins CI 和 LTS 远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://wiki.jenkins-ci.org/display/SECURITY/Security+Advisory+2016-02-24
CNVD-2016-01391	JasPer 'jas_matrix_create()'函数远程整数溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.ece.uvic.ca/~frodo/software.html
CNVD-2016-01390	Linux kernel 本地权限提升漏洞（CNVD-2016-01390）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.kernel.org/
CNVD-2016-01389	OIC Exponent CMS 远程代码执行漏洞	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.exponentcms.org/
CNVD-2016-01388	QNAP Systems iArtist Lite 命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.qnap.com/
CNVD-2016-01385	QNAP Systems Signage Station 脚本执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.qnap.com/

表 4 部分重要高危漏洞列表

小结：本周，OpenSSL 产品被披露存在多个安全漏洞，攻击者利用漏洞可进行跨协议攻击和发起拒绝服务攻击等。此外，IBM、Wireshark、Yeager 等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、执行任意代码、进行跨站脚本和跨站

请求伪造攻击或发起拒绝服务攻击等。此外，ZOHO ManageEngine Firewall Analyzer 被披露存在一个 SQL 注入漏洞，攻击者可利用该漏洞控制应用程序，访问或修改数据库数据。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. Jenkins 之 Java 反序列化漏洞

Jenkins 近日修复了一个可通过低权限用户调用 API 服务致使的命令执行漏洞：低权限用户通过构造一个恶意的 XML 文档并发送至服务端接口，使服务端解析时调用 API 执行外部命令。因此，对于 jenkins 用户，我们给予以下安全建议：1、Jenkins 已经发布了该漏洞的补丁，建议用户更新至最新版本 Jenkins 1.650 及以上版本，并且尽量保证 jenkins 账号不为弱口令。2、网络管理员应该对 jenkins 实行访问控制，并且放入内网对外网不开放，同时禁止 jenkins 的匿名访问权限。

参考链接：http://www.freebuf.com/vuls/97659.html

2. 安卓版百度浏览器远程代码执行漏洞

近日，安全研究人员在百度安卓浏览器中，发现了一个远程代码执行漏洞。由于 Windows 和安卓版本的百度浏览器，都未使用代码签名机制来保护软件更新的安全。这意味着在其程序路径下的恶意文件可以下载并执行任意代码，系统将存在巨大的隐患。

参考链接：http://www.freebuf.com/vuls/97607.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