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 22 日-2016 年 02 月 28 日 **2016 年第 9 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 160 个，其中高危漏洞 37 个、中危漏洞 115 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 147 个。本周收录的漏洞中，已有 141 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“GraphicsMagick 缓冲区溢出漏洞”、“Enhancesoft osTicket 任意文件上传漏洞”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 160 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、绿盟科技、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 690 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)	63	63
启明星辰	283	1
天融信	148	0
安天实验室	73	0
绿盟科技	84	0
恒安嘉新	67	0

H3C	4	0
乌云	538	538
漏洞盒子	30	30
CNCERT 江西分中心	12	12
CNCERT 安徽分中心	5	5
个人	41	41
报送总计	1348	690
录入总计	160（去重）	690

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cybozu、Cisco、Apache 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	Cybozu	16	10%
2	Cisco	11	7%
3	Apache	8	5%
4	IBM	7	4%
5	Microsoft	6	4%
6	Ipswitch	5	3%
7	Xymon	5	3%
8	Symantec	4	3%
9	D-Link	3	2%
10	其他	95	59%

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 160 个漏洞。其中应用程序漏洞 114 个，Web 应用漏洞 21 个，网络设备漏洞 13 个，安全产品漏洞 6 个，操作系统漏洞 4 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	114
Web 应用漏洞	21

网络设备漏洞	13
安全产品漏洞	6
操作系统漏洞	4
数据库漏洞	2

表 3 漏洞按影响类型统计表

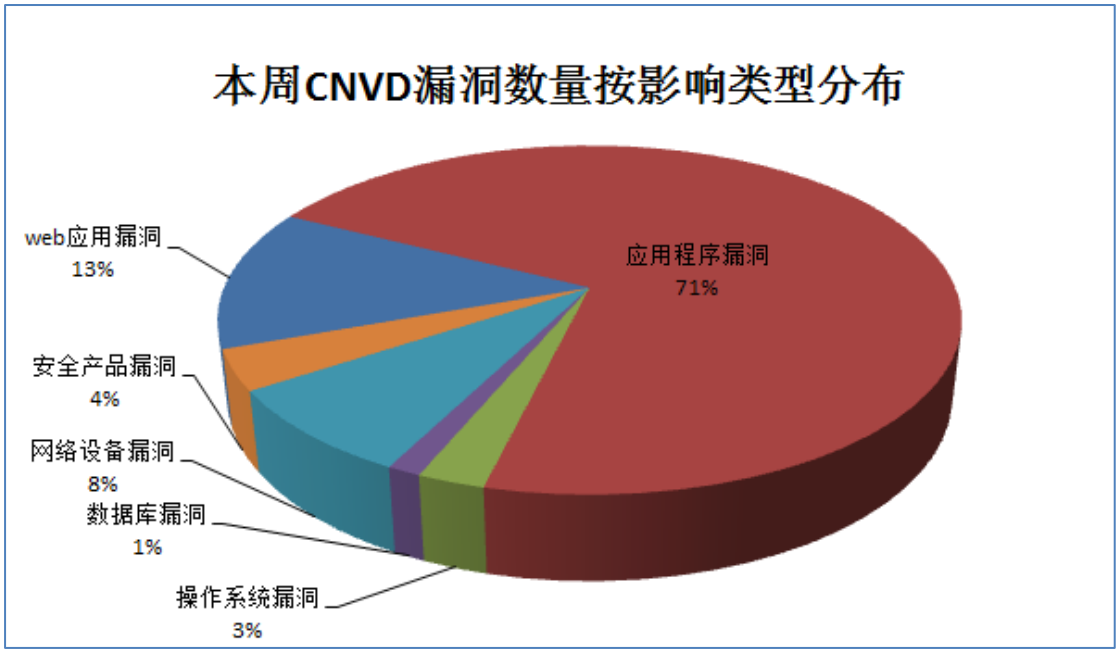

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 17 个电信行业漏洞（如下图表所示）。其中，“PostgreSQL 权限提升漏洞、ZOHO ManageEngine Network Configuration Manager 权限提升漏洞、IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2016-01275、CNVD-2016-01273、CNVD-2016-01274）、Belden Hirschmann Classic Platform switches L2B 信息泄露漏洞”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-2016-01164	D-Link DVG-N5402SP 目录遍历漏洞	中	否
电信	CNVD-2016-01162	D-Link DVG-N5402SP 信息泄露漏洞	中	否
电信	CNVD-2016-01171	PostgreSQL 拒绝服务漏洞（PostgreSQL 拒绝服务漏洞）	中	是
电信	CNVD-2016-01172	PostgreSQL 权限提升漏洞	高	是
电信	CNVD-2016-01177	Cisco Prime Collaboration CLI 命令执行漏洞	中	是
电信	CNVD-2016-01189	Viprinet Europe Multichannel VPN Router 300 协议降级漏洞	中	是
电信	CNVD-2016-01188	Viprinet Europe Multichannel VPN Route	中	是

		r 300 中间人攻击漏洞		
电信	CNVD-2016-01187	Viprinet Europe Multichannel VPN Router 300 跨站脚本漏洞	中	是
电信	CNVD-2016-01211	Cisco IOS 拒绝服务漏洞（CNVD-2016-01211）	中	是
电信	CNVD-2016-01221	ZOHO ManageEngine Network Configuration Manager 权限提升漏洞	高	是
电信	CNVD-2016-01255	ASUS RT-N56U HTML 注入漏洞	中	否
电信	CNVD-2016-01275	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2016-01275）	高	是
电信	CNVD-2016-01273	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2016-01273）	高	是
电信	CNVD-2016-01274	IBM Tivoli Storage Manager FastBack 栈缓冲区溢出漏洞（CNVD-2016-01274）	高	是
电信	CNVD-2016-01326	Apache Tomcat 目录遍历漏洞	中	是
电信	CNVD-2016-01325	Apache Tomcat 跨站请求伪造漏洞（CNVD-2016-01325）	中	是
电信	CNVD-2016-01335	Belden Hirschmann Classic Platform switches L2B 信息泄露漏洞	高	是

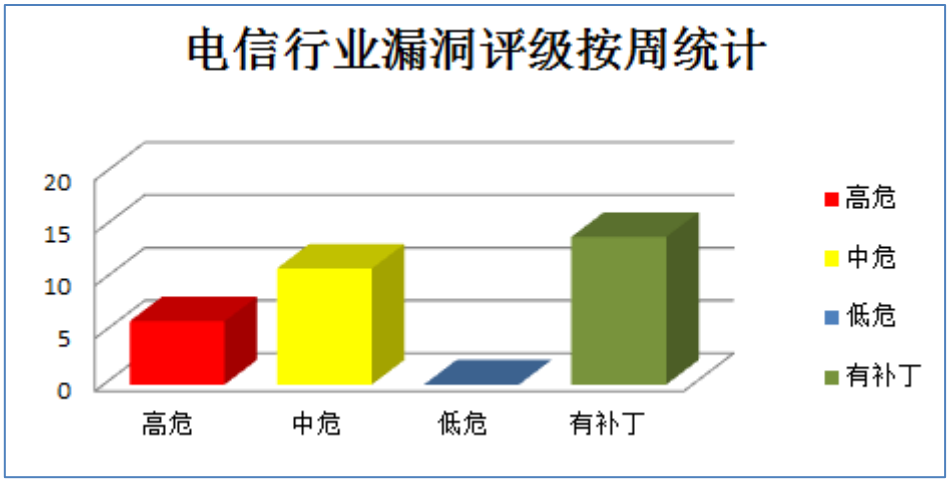

图 1 电信行业漏洞统计

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 StarOS on ASR 5000 是美国思科（Cisco）公司的一套运行于 5000 系列路由器设备中的操作系统。Cisco NX-OS 是美国思科（Cisco）公司的一个数据中心级的操作系统，该操作系统体现了模块化设计、永续性和可维护性。Cisco Spark 是一套协同

合作服务解决方案。Cisco Prime Collaboration 是一套企业协作网络管理解决方案。Cisco Email Security Appliance 是一款是广泛使用的邮件加密网关，能够无缝地完成机密电子邮件的加密、解密和数字签名工作。Cisco Application Policy Infrastructure Controller Enterprise 是一款应用策略架构控制模块。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获取提升权限、进行跨站攻击、发起拒绝服务攻击或执行命令等。

CNVD 收录的相关漏洞包括：Cisco StarOS 权限提升漏洞、Cisco NX-OS 权限提升漏洞、Cisco Spark REST 接口拒绝服务漏洞、Cisco Spark REST 接口访问绕过漏洞、Cisco Spark REST 接口信息泄露漏洞、Cisco Prime Collaboration CLI 命令执行漏洞、Cisco Email Security Appliance 安全绕过漏洞、Cisco Application Policy Infrastructure Controller Enterprise 模块跨站脚本漏洞。其中，“Cisco StarOS 权限提升漏洞”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-2016-01313
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01317
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01199
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01181
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01198
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01177
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01173
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01216

2、 Cybozu 产品安全漏洞

Cybozu Office 是日本 Cybozu 公司开发的一款基于 WEB 的跨平台办公室解决方案。本周，上述产品被披露存在安全机制绕过和跨站脚本漏洞。攻击者利用漏洞可绕过安全机制和进行跨站攻击。

CNVD 收录的相关漏洞包括：Cybozu Office 安全机制绕过漏洞（CNVD-2016-01257、CNVD-2016-01259、CNVD-2016-01258、CNVD-2016-01260）、Cybozu Office 跨站脚本漏洞（CNVD-2016-01251、CNVD-2016-01252、CNVD-2016-01250、CNVD-2016-01249）。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-2016-01257
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01259
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01258
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01260
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01251
http://www.cnvd.org.cn/flaw/show/CNVD-2016-01252

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01250

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01249

3、Symantec 产品安全漏洞

Symantec Encryption Management Server 可以管理并自动化加密解决方案的安全策略。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、提升权限、执行任意命令和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Symantec Encryption Management Server (SEMS) 远程拒绝服务漏洞、Symantec Encryption Management Server (SEMS) 本地权限提升漏洞、Symantec Encryption Management Server (SEMS) OS 远程命令执行漏洞、Symantec Encryption Management Server (SEMS) 远程信息泄露漏洞。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-2016-01220

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01219

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01218

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01217

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Graphite 是一套使用 Python 语言编写、采用 Django 框架的企业级开源系统监控工具，它通过第三方工具或插件进行数据收集、统计，最后完成数据绘图。Graphite 2 是 Graphite 的一个升级版。本周，上述产品被披露存在任意代码执行和拒绝服务漏洞，攻击者利用漏洞可执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR Graphite 2 TtfUtil.cpp 文件拒绝服务漏洞、Mozilla Firefox 和 Firefox ESR Graphite 2 FeatureMap.cpp 文件拒绝服务漏洞、Mozilla Firefox 和 Firefox ESR Graphite 2 Code.cpp 文件拒绝服务漏洞、Mozilla Firefox 和 Firefox ESR Graphite 2 任意代码执行漏洞。其中，“Mozilla Firefox 和 Firefox ESR Graphite 2 任意代码执行漏洞”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-2016-01202

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01201

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01200

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01180

5、D-Link DVG-N5402SP 权限获取漏洞

D-Link DVG-N5402SP 是友讯（D-Link）公司的一款通过 IP 网络进行语音、传真和

共享无线互联网的无线路由器产品。本周，D-Link DVG-N5402SP 被披露存在权限获取漏洞，攻击者可利用漏洞获取管理员控制权限。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-2016-01163

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-2016-01167	Microsoft Windows Journal 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：https://technet.microsoft.com/en-us/library/security/ms16-013.aspx
CNVD-2016-01174	EMC Documentum xCP SQL 查询注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.emc.com/
CNVD-2016-01210	Citrix Systems NetScaler Application Delivery Controller 和 NetScaler Gateway 权限获取漏洞	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://support.citrix.com/article/CTX206001
CNVD-2016-01221	ZOHO ManageEngine Network Configuration Manager 权限提升漏洞	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.manageengine.com/
CNVD-2016-01227	libpng ‘pngwutil.c’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.libpng.org/
CNVD-2016-01222	QEMU 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://wiki.qemu.org/Main_Page
CNVD-2016-01230	多款 Dell 产品任意命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.software.dell.com/product-notification/185943
CNVD-2016-01229	多款 Dell 产品任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.software.dell.com/product-notification/185943
CNVD-2016-01245	Google Chrome 任意代码执行漏洞（CNVD-2016-01245）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://googlechromereleases.blogspot.com/2016/02/stable-channel-update_

			9.html
CNVD-2016-01287	Xymon HTML 注入漏洞	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://xymon.sourceforge.net/

表 3 部分高危漏洞列表

小结：本周，Cisco 被披露存在多个安全漏洞，攻击者利用漏洞可获取提升权限、进行跨站攻击、发起拒绝服务攻击或执行命令等。另外，Cybozu、Symantec、Mozilla 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、提升权限、进行跨站攻击、执行任意代码和发起拒绝服务攻击等。此外，D-Link DVG-N5402SP 被披露存在一个高危漏洞，攻击者可利用漏洞获取管理员控制权限。

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、Huawi 修补 Policy Center 和 Mate S 产品漏洞

Huawei Policy Center 是华为公司的一套策略管理中心软件。Huawei Mate S 是中国华为公司的一款智能手机产品。

本周，Huawei 修补了上述产品存在的权限提升和整数溢出漏洞，避免攻击者利用漏洞提升权限和执行任意代码。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/71819

http://www.cnvd.org.cn/patchInfo/show/71804

本周要闻速递

1. aswSnx.sys 中的内核分页池缓冲区溢出漏洞

近日，Nettitude 安全人员在 Avast Virtualization 内核模式驱动(aswSnx.sys)中发现一个安全漏洞，使用普通账户登录的本地攻击者可利用该漏洞提升权限，以系统权限执行任意代码，进而完全控制受影响主机。其受影响产品及版本如下：Avast InternetSecurity v11.1.2245、Avast ProAntivirus v11.1.2245、Avast Premierv11.1.2245、Avast FreeAntivirus v11.1.2245。且上述产品中的早期版本也可能受到影响。

参考链接：http://www.freebuf.com/vuls/96572.html

2. 大批 WordPress 网站被渗透 ，成为 DDOS 攻击源

近日，Sucuri 的安全研究人员发现，数万 WordPress 站点被利用于实施第 7 层 DDos 攻击。共有两万六千个不同的 WordPress 站点持续向同一个网站以每秒一万到一万一

千次的频率发送 HTTPS 请求，最多时能达到两万次每秒。更严重是，如果 Pingback 功能默认开启，全球任何一个 WordPress 站点都可能被利用，成为 DDos 攻击网络的一个源头。HTTP Flood 是针对 Web 服务在第七层协议发起的大规模流量攻击，不仅可以直接导致被攻击的 Web 前端响应缓慢，还间接攻击到后端的 Java 等业务层逻辑以及更后端的数据库服务，增大它们的压力，甚至对日志存储服务器都带来影响。建议所有基于 Wordpress 的网站尽快禁用 Pingback。虽然无法保证网站免于遭受攻击，但会终止黑客利用您的网站来攻击其它目标。

参考链接：http://www.freebuf.com/news/96845.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