国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 10 月 10 日-2016 年 10 月 16 日 **2016 年第 42 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 255 个，其中高危漏洞 85 个、中危漏洞 151 个、低危漏洞 19 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 90 个（占 36%）。其中互联网上出现“FreePBX 远程命令执行漏洞（CNVD-2016-08542）、NetMan 204 后门账户漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。此外，本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 768 个，与上周（1517 个）环比下降 50%。

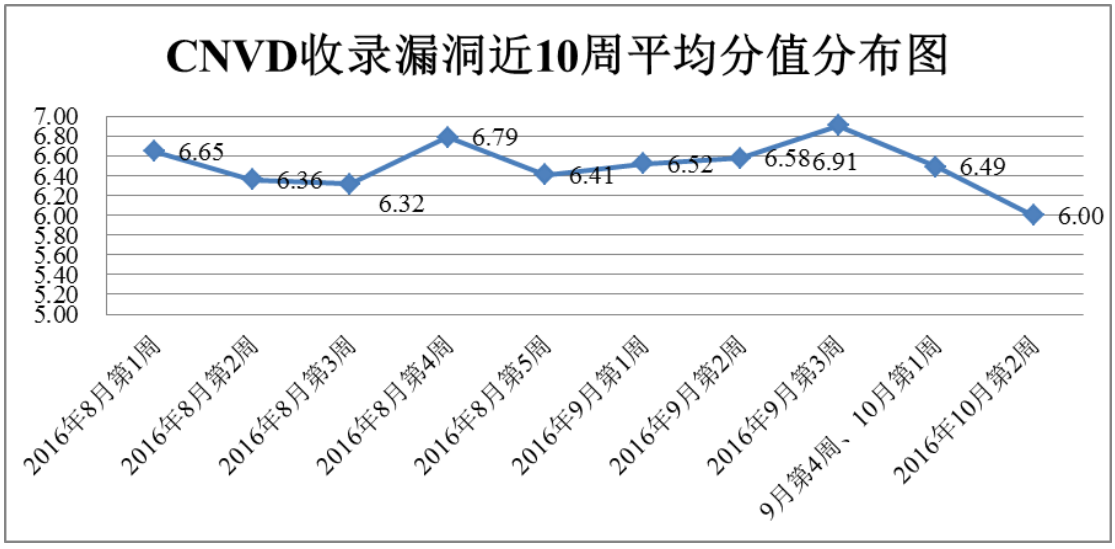

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 255 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信、蓝盾信息安全技术有限公司等单位报送数量较多。奇虎（补天平台）、漏洞盒子、腾讯玄武实验室、西安四叶草信息技术有限公司、深圳市深信服电子科技有限公司、广西鑫瀚科技有限公

司、广州神月信息安全技术有限公司、广州圣辉信息技术有限公司、上海零盾网络科技有限公司及其他个人白帽子向 CNVD 提交了 768 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）	561	561
启明星辰	259	0
安天实验室	203	0
天融信	196	0
蓝盾信息安全技术有限公司	139	0
杭州安恒信息技术有限公司	94	18
恒安嘉新	96	5
H3C	28	0
中国电信集团系统集成有限责任公司	26	0
东软	6	6
漏洞盒子	81	81
腾讯玄武实验室	26	26
西安四叶草信息技术有限公司	17	17
深圳市深信服电子科技有限公司	9	9
广西鑫瀚科技有限公司	5	5
广州神月信息安全技术有限公司	2	2
广州圣辉信息技术有限公司	2	2
上海零盾网络科技有限公司	2	2
个人	34	34
报送总计	1786	768

录入总计	255（去重）	768

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 255 个漏洞。其中应用程序漏洞 132 个，web 应用漏洞 89 个，网络设备漏洞 20 个，操作系统漏洞 9 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	132
web 应用漏洞	89
网络设备漏洞	20
操作系统漏洞	9
安全产品漏洞	5

表 2 漏洞按影响类型统计表

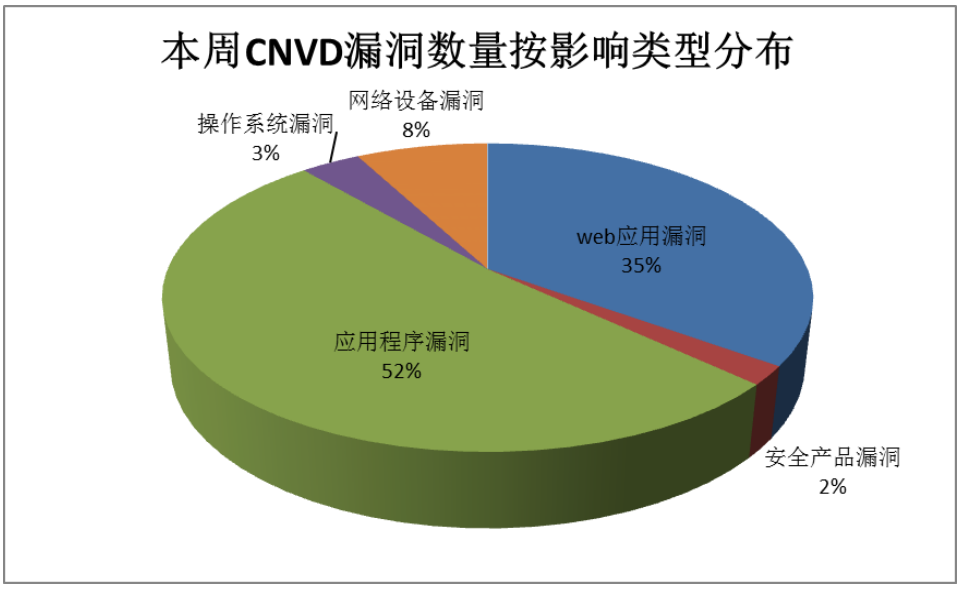

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 X.Org、BaserCMS、Microsoft 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	X.Org	13	5%
2	BaserCMS	12	5%
3	Microsoft	9	4%
4	ImageMagick	9	4%
5	Cybozu	8	3%
6	Cisco	7	3%

7	ffmpeg	7	3%
8	Siemens	6	2%
9	PHPCMS	6	2%
10	其他	178	69%

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 1 个电信行业漏洞，1 个移动互联网行业漏洞，8 个工控系统行业漏洞（如下图所示）。其中，“Auto-Matrix Aspect-Nexus 和 Aspect-Matrix Building Automation Front-End Solutions 信息泄露漏洞、Auto-Matrix Aspect-Nexus 和 Aspect-Matrix Building Automation Front-End Solutions 文件包含漏洞、Beckhoff Embedded PC 图像和 Automation Device Specification TwinCAT 组件安全绕过漏洞（CNVD-2016-08764）、Beckhoff Embedded PC 图像和 Automation Device Specification TwinCAT 组件安全绕过漏洞”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/

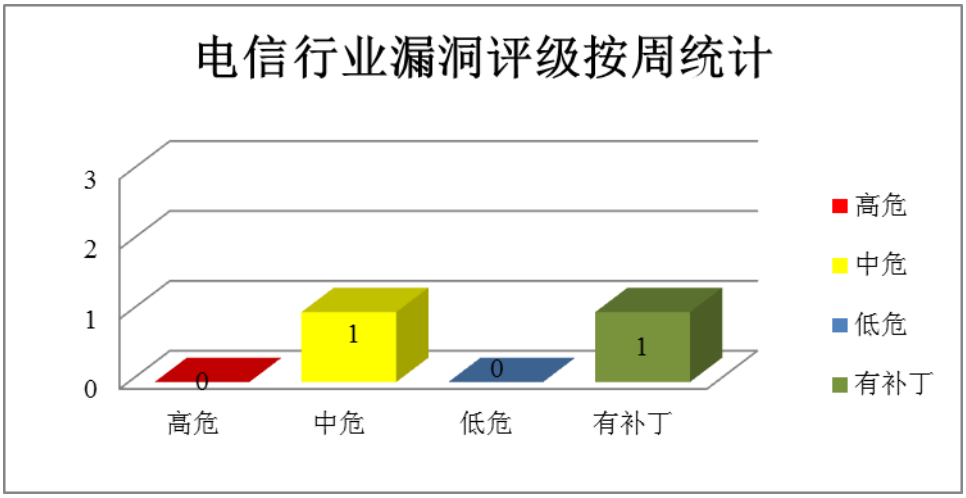

图 3 电信行业漏洞统计

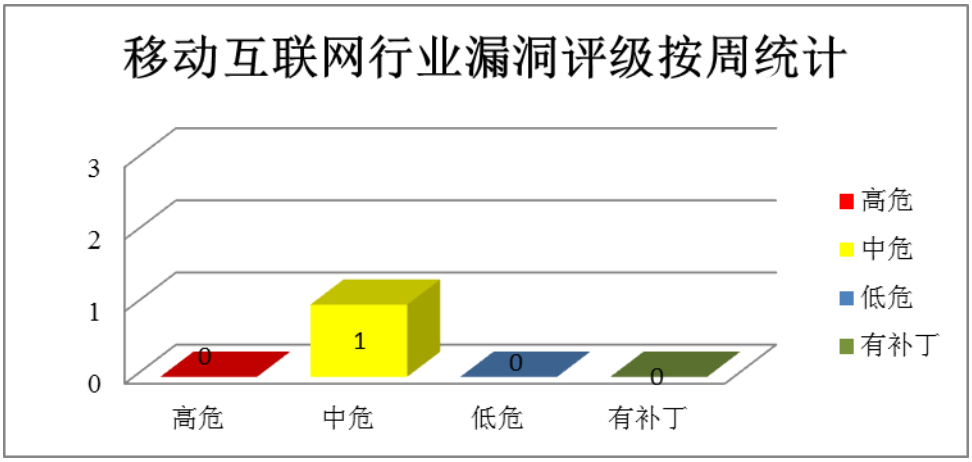

图 4 移动互联网行业漏洞统计

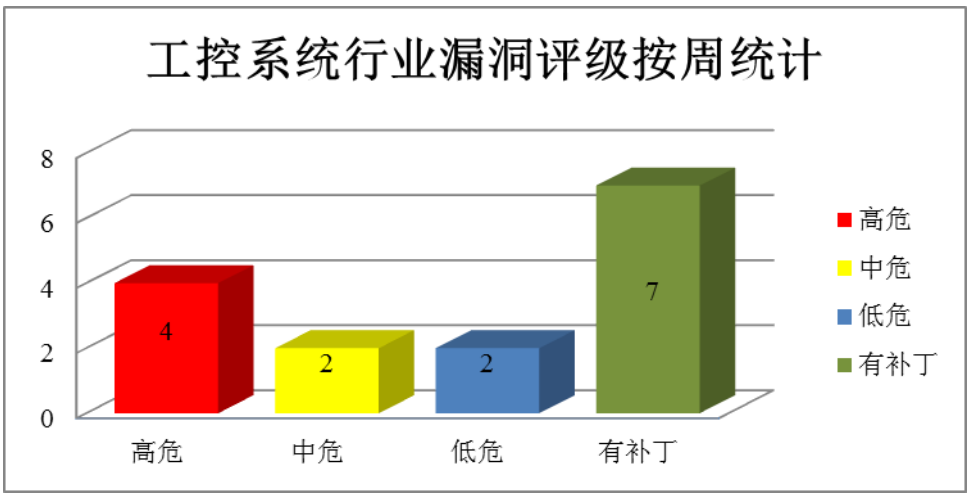

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

10 月 11 日，微软发布了 2016 年 10 月份的月度例行安全公告，共含 10 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Office、Office Services 、.NET Framework、Lync 和 Skype for Business、Web Apps、Adobe Flash Player 中存在的 36 个安全漏洞。其中，5 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。CNVD 提醒广大 Microsoft 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。

CNVD 收录的相关漏洞包括：Microsoft Windows Video Control 远程代码执行漏洞、Microsoft Internet Explorer 和 Edge 远程权限提升洞、Microsoft Windows 内核 Win32k 特权提取漏洞、Microsoft Windows Diagnostics Hub 本地权限提升漏洞、Microsoft Edge 脚本引擎信息泄露漏洞、Microsoft Edge 安全绕过漏洞、Microsoft Internet Explor

er 远程信息泄露漏洞、Microsoft Internet Explorer 和 Edge 远程内存破坏漏洞等。除“Microsoft Edge 脚本引擎信息泄露漏洞、Microsoft Edge 安全绕过漏洞、Microsoft Internet Explorer 远程信息泄露漏洞”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/webinfo/show/3945

2、X.Org 产品安全漏洞

X.Org libXi 是 X.Org 基金会运作的一个 X 输入扩展库。X.Org libX11 是一个 X11（X Window 系统）客户端库。X.Org libXv 是一个 X Video 扩展专属的基于 Xlib 的客户端库。X.Org libXvMC 是一个 X-Video Motion Compensation API 专属的基于 Xlib 的客户端库。X.Org libXrender 是一个 Render 扩展专属的轻量级的库接口。本周，上述产品被披露存拒绝服务和内存破坏漏洞，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：X.Org libXi 拒绝服务漏洞、X.Org libXi 拒绝服务漏洞（CNVD-2016-08890）、X.Org libX11 拒绝服务漏洞、X.Org libX11 拒绝服务漏洞（CNVD-2016-08893）、X.Org libXv 内存破坏漏洞、X.Org libXvMC 内存破坏漏洞、X.Org libXrender 拒绝服务漏洞、X.Org libXrender 拒绝服务漏洞（CNVD-2016-08886）等。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-2016-08889
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08890
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08892
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08893
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08894
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08882
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08885
http://www.cnvd.org.cn/flaw/show/CNVD-2016-08886

3、Cisco 产品安全漏洞

Cisco Unified Contact Center Express（Unified CCX）和 Cisco Unified Intelligence Center（CUIC）都是美国思科（Cisco）公司的产品。Cisco Nexus 7000 Series Switches 是一个模块化数据中心级产品系列。Cisco Firepower Management Center 是新一代防火墙管理中心软件。Cisco IOS XR Software 是 IOS 软件系列（包括 IOS T、IOS S 和 IOS XR）中的一套完全模块化、分布式的网络操作系统。本周，上述产品被披露存在多个漏洞漏洞，攻击者可利用漏洞造成跨站脚本攻击、远程执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Unified Intelligence Center 跨站脚本漏洞、Cisco Nexus 7000/7700 OTV 缓冲区溢出漏洞、Cisco Firepower Management Center Cons

ole 本地文件包含漏洞、Cisco Firepower Threat Management Console 拒绝服务漏洞、Cisco Firepower Threat Management Console 远程命令执行漏洞、Cisco Firepower Management Center Console 认证绕过漏洞、Cisco IOS XR Software 拒绝服务漏洞（CNVD-2016-08560）等。其中，“Cisco Nexus 7000/7700 OTV 缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco Firepower Threat Management Console 拒绝服务漏洞、Cisco IOS XR Software 拒绝服务漏洞（CNVD-2016-08560）”外漏洞的修补程序。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-2016-08872

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08613

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08559

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08895

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08609

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08561

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08560

4、ImageMagick 产品安全漏洞

ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图象处理软件。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：ImageMagick 拒绝服务漏洞（CNVD-2016-08638、CNVD-2016-08684、CNVD-2016-08683、CNVD-2016-08682、CNVD-2016-08639）、ImageMagick 'coders/viff.c'拒绝服务漏洞、imagemagick mogrify 拒绝服务漏洞、ImageMagick ‘MagickCore/memory.c’拒绝服务漏洞等。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-2016-08638

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08684

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08683

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08682

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08639

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08693

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08722

http://www.cnvd.org.cn/flaw/show/CNVD-2016-08531

5、北京三维天地物资供应资源管理信息系统 xxbh 参数存在 SQL 注入漏洞

物资供应资源管理信息系统是一款在国内外先进的现代化企业管理理论和管理方法的基础上发展起来的企业管理软件。本周，北京三维天地物资供应资源管理信息系统被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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-2016-08701

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-2016-08533	Fortinet FortiClient DLL 加载远程代码执行漏洞	高	用户可联系供应商获得补丁信息：http://www.forticlient.com/
CNVD-2016-08539	Joomla! Component Event Booking 组件 SQL 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://extensions.joomla.org
CNVD-2016-08612	EMC Replication Manager 和 EMC Networker Module for Microsoft 远程代码执行漏洞	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.emc.com/
CNVD-2016-08712	Apple OS X IOThunderboltFamily 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.apple.com/HT207170
CNVD-2016-08713	Apple OS X Apple HSSPI Support 内存破坏漏洞	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.apple.com/HT207170
CNVD-2016-08714	Apple OS X AppleUUC 内存破坏漏洞	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.apple.com/HT207170
CNVD-2016-08715	Apple OS X AppleUUC 内存破坏漏洞（CNVD-2016-08715）	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.apple.com/HT207170
CNVD-2016-08760	U by BBT for iOS 安全绕过漏洞	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：https://www.bbt.com/
CNVD-2016-08761	EMC Unisphere for VMAX Virtual Appliance 和 Solutions Enabler Virtual Appliance 任意命令执行漏洞	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.emc.com/
CNVD-2016-08762	EMC Unisphere for VMAX Virtual Appliance 和 Solutions Enabler Virtual Appliance 任意命令执行漏洞（CNVD-2016-08762）	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.emc.com/

表 4 部分重要高危漏洞列表

10 月 11 日，微软发布了 2016 年 10 月份的月度例行安全公告，共含 10 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Office、Office Services 、.NET Framework、Lync 和 Skype for Business、Web Apps、Adobe Flash Player 中存在多个安全

漏洞，攻击者可提升权限，远程执行任意代码。此外， X.Org、Cisco、ImageMagick 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行未授权操作等。另外，北京三维天地物资供应资源管理信息系统被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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.漏洞预警：基于 RedHat 发行的 Apache Tomcat 本地提权漏洞

2016 年 10 月 11 日，网上爆出 Tomcat 本地提权漏洞，漏洞编号为 CVE-2016-5425。此次受到影响的主要是基于 RedHat 发行版 Apache Tomcat，包括 CentOS，RedHat，OracleLinux，Fedora 等等。主要原因是普通 Tomcat 用户拥有权限来对/usr/lib/tmpfiles.d/tomcat.conf 这个配置文件进行读写，那么该用户组成员或者拥有普通 Tomcat 权限的 Web Shell 可以将权限提升至 root 级别。Redhat 安全小组已经在第一时间修复了受影响的 Tomcat 上游包,直接更新发行版提供的 Tomcat 即可。

参考链接：http://www.freebuf.com/news/116412.html

2. PHP7.0.0 格式化字符串漏洞与 EIP 劫持分析

vspprintf()函数在 zend_throw_error()函数中，当触发漏洞时，zend_throw_error()函数由 zend_throw_or_error()函数调用。由于调用时少了一个参数导致触发了格式化字符串漏洞。可以分别在 windows 和 linux 两种不同的环境下，运用该漏洞劫持 EIP。

参考链接：http://www.freebuf.com/vuls/116115.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