

信息安全漏洞周报

2016 年 12 月 12 日-2016 年 12 月 18 日

2016年第51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 274 个，其中高危漏洞 98 个、中危漏洞 164 个、低危漏洞 12 个。漏洞平均分为 6.29。本周收录的漏洞中，涉及 0day 漏洞 42 个（占 15%）。其中互联网上出现“网件 Netgear 多款路由器存在任意命令注入漏洞、Microsoft PowerShell XML 外部实体注入漏洞”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 734 个，与上周（1054 个）环比下降 30%。

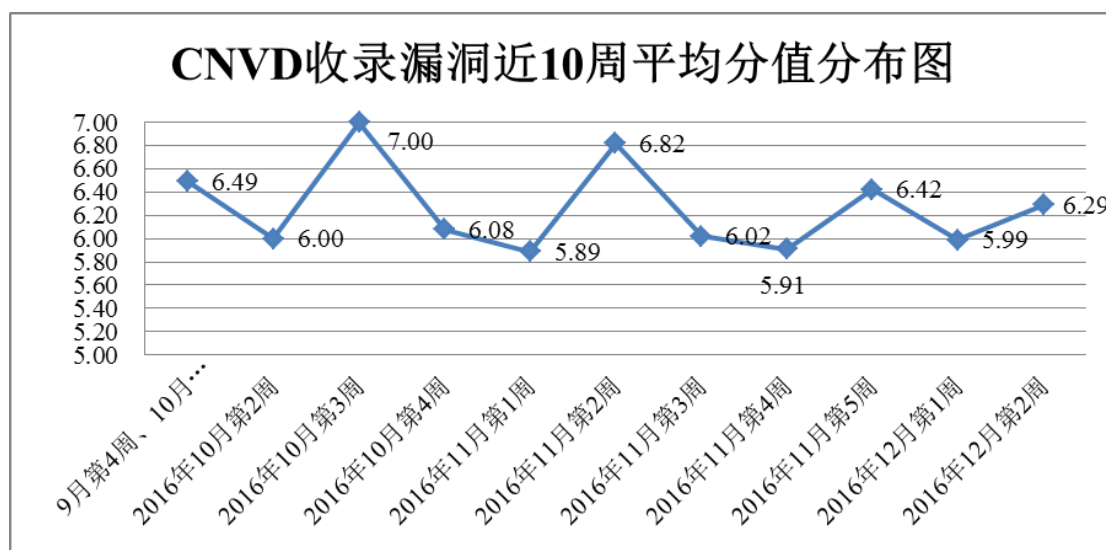


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 12 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 274 漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、蓝盾信息安全技术股份有限公司、恒安嘉新报送数量较多。360 网神、漏洞盒子、南京铤迅信息技术股份有限

公司、北京安码科技有限公司及其他个人白帽子向 CNVD 提交了 734 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
360 网神	578	578
安天实验室	220	0
启明星辰	200	4
蓝盾信息安全技术股份有限公司	119	0
恒安嘉新	119	0
华为技术有限公司	104	0
H3C	84	0
天融信	70	0
杭州安恒信息技术有限公司	56	1
绿盟科技	23	0
北京数字观星科技有限公司	5	0
南京铨迅信息技术股份有限公司	2	2
漏洞盒子	77	77
北京安码科技有限公司	2	2
CNCERT 宁夏分中心	1	1
CNCERT 江西分中心	1	1
个人	76	76
报送总计	1414	734
录入总计	274（去重）	734

表 1 漏洞报送情况统计表

本周，CNVD 收录了 274 个漏洞。其中应用程序漏洞 146 个，操作系统漏洞 76 个，web 应用漏洞 27 个，网络设备漏洞 19 个，安全产品漏洞 4 个，数据库漏洞 2 条。

漏洞影响对象类型	漏洞数量
应用程序漏洞	146
操作系统漏洞	76
web 应用漏洞	27
网络设备漏洞	19
安全产品漏洞	4
数据库漏洞	2

表 2 漏洞按影响类型统计表

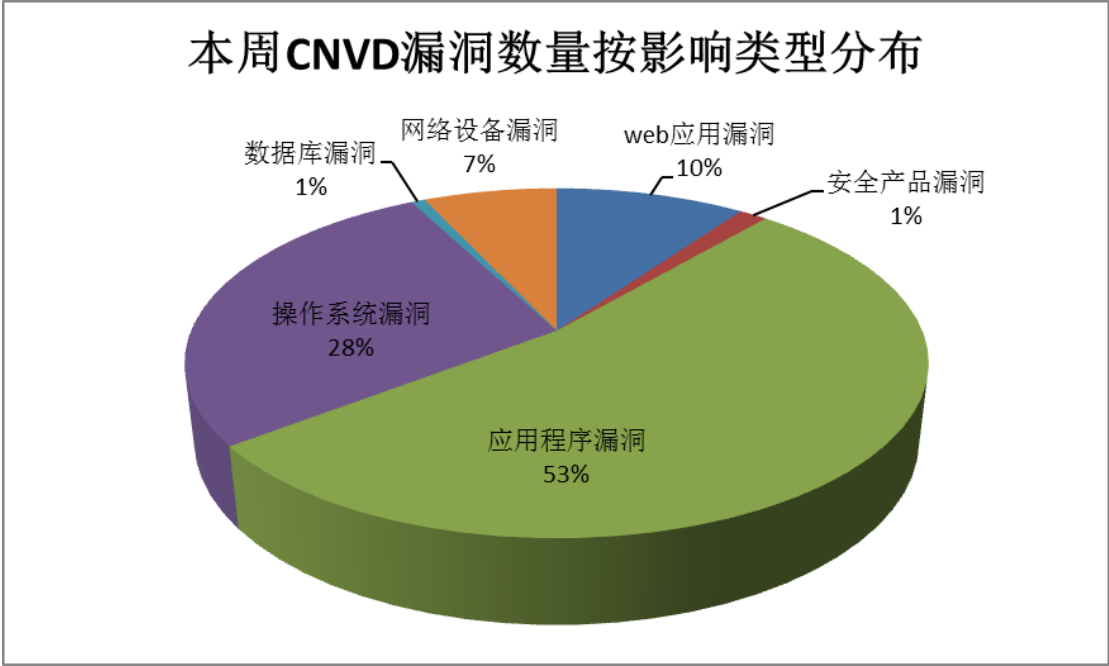


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Adobe 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	Google	87	32%
2	Microsoft	43	16%
3	Adobe	23	8%
4	Cisco	11	4%
5	WordPress	9	3%
6	Libav	8	3%
7	PHP	5	2%

8	Huawei	4	1%
9	BlueZ	4	1%
10	其他	80	30%

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 7 个电信行业漏洞，62 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Google Nexus NVIDIA GPU Driver 权限提升漏洞、Google Nexus NVIDIA GPU Driver 权限提升漏洞（CNVD-2016-12230、CNVD-2016-12231）、Google Nexus Qualcomm Sound 驱动程序权限提升漏洞（CNVD-2016-12200、CNVD-2016-12201）、Google Android Telephony 权限提升漏洞、Google Android Framework API 权限提升漏洞、Google Android Wi-Fi 权限提升漏洞、Google Android Broadcom Wi-Fi Driver 权限提升漏洞、Google Nexus Qualcomm MSM 权限提升漏洞”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/>

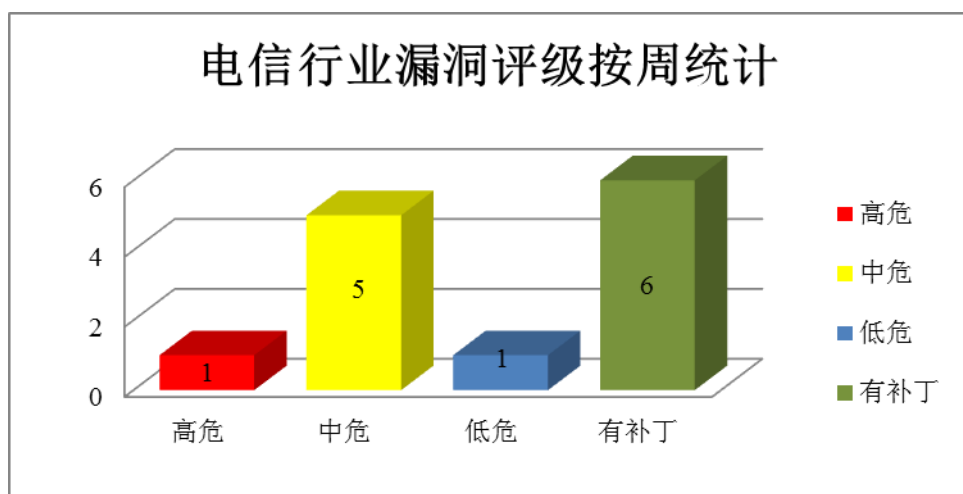


图 3 电信行业漏洞统计

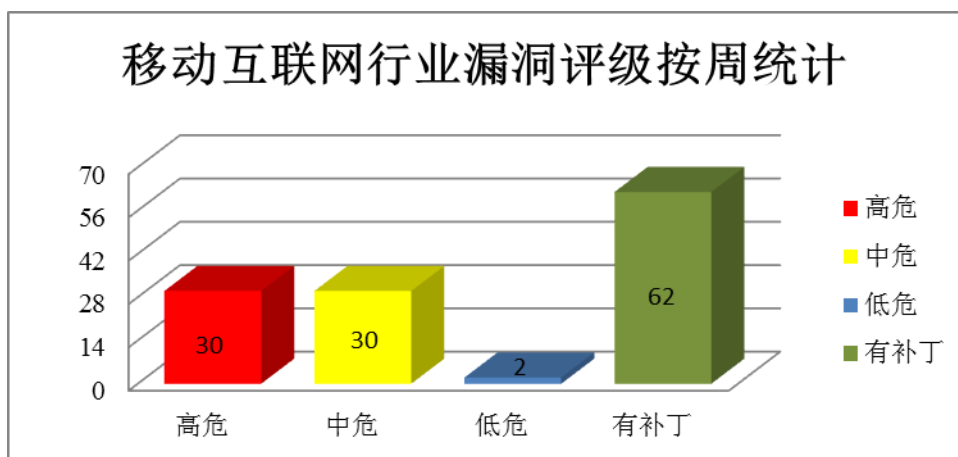


图 4 移动互联网行业漏洞统计

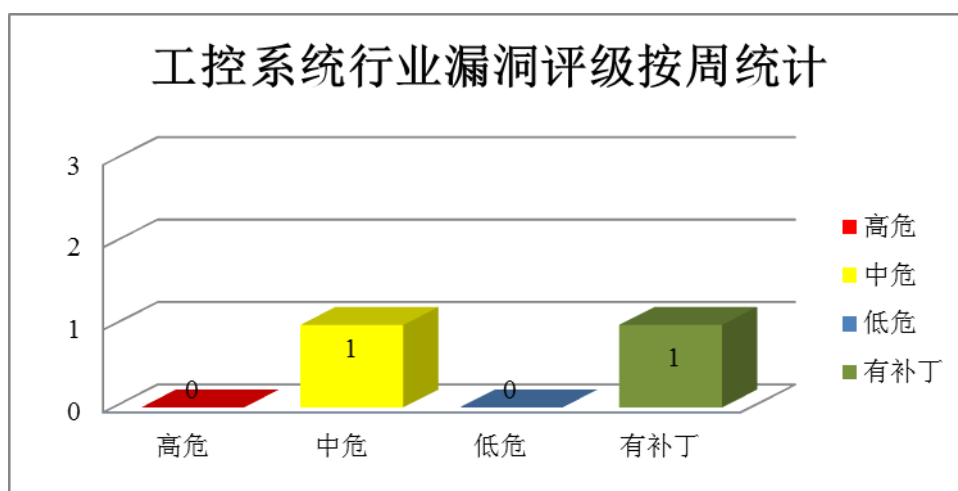


图 5 工控系统行业漏洞统计

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

12 月 13 日，微软发布了 2016 年 12 月份的月度例行安全公告，共含 12 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Office、Office Services、.NET Framework 和 Web Apps 中存在的 41 个安全漏洞。其中，6 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 Office 内存破坏漏洞（CNVD-2016-12457、CNVD-2016-12456、CNVD-2016-12455、CNVD-2016-12454）、Microsoft Edge 内存破坏漏洞（CNVD-2016-12447、CNVD-2016-12448、CNVD-2016-12449、CNVD-2016-12452）等。上述漏洞的综合评级为“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/4010>

2、Google 产品安全漏洞

Android 和 Android on Google Pixel XL 等都是美国谷歌 (Google) 公司和开放手持设备联盟 (简称 OHA) 共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm Media Codecs 是其中的一个高通多媒体编解码器组件。MediaTek Driver 是使用在其中的一个联发科 (MediaTek) 公司的设备专用的联发科驱动组件。本周, 上述产品被披露存在权限提升漏洞, 攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括: Google Android MediaTek 驱动程序权限提升漏洞 (CNVD-2016-12190、CNVD-2016-12189、CNVD-2016-12188、CNVD-2016-12187)、Google Android MediaTek 驱动程序权限提升漏洞、Google Nexus Qualcomm Media Codecs 权限提升漏洞 (CNVD-2016-12167、CNVD-2016-12168、CNVD-2016-12169) 等。上述漏洞的综合评级为“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-2016-12190>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12189>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12188>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12187>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12186>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12167>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12168>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12169>

3、Adobe 产品安全漏洞

Adobe Flash Player 是美国 Adobe 公司开发的一款广泛使用的、专有的多媒体程序播放器。本周, 该产品被披露存在内存破坏和代码执行漏洞, 攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括: Adobe Flash Player 内存破坏漏洞 (CNVD-2016-12384、CNVD-2016-12383、CNVD-2016-12382、CNVD-2016-12381、CNVD-2016-12380)、Adobe Flash Player 代码执行漏洞 (CNVD-2016-12359、CNVD-2016-12358、CNVD-2016-12357) 等。上述漏洞的综合评级为“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-2016-12384>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12383>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12382>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12381>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12380>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12359>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12358>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12357>

4、Cisco 产品安全漏洞

Cisco IOS 和 IOS XE Software 都是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco IOx 是一套为思科物联网网络基础设施（提供统一托管功能的应用程序。Cisco Emergency Responder（ER）是一套 IP 通信系统中的应急呼叫软件。Cisco AsyncOS for Web Security Appliance（WSA）是一套网络安全设备。Cisco AsyncOS 是一套使用在这个产品中的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco IOS Frame Forwarding 拒绝服务漏洞、Cisco IOS XR Software 默认账户密码漏洞、Cisco IOS and IOS XE Software 安全绕过漏洞、Cisco IOS XR Software 拒绝服务漏洞（CNVD-2016-12410）、Cisco IOS and IOS XE Software 路径遍历漏洞、Cisco Emergency Responder 跨站请求伪造漏洞、Cisco IOS 和 IOS XE Software 身份验证绕过漏洞、Cisco AsyncOS 远程拒绝服务漏洞等。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-2016-12408>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12409>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12407>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12410>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12428>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12388>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12229>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12228>

5、Microsoft PowerShell XML 外部实体注入漏洞

Microsoft PowerShell 是运行在 windows 机器上实现系统和应用程序管理自动化的命令行脚本环境。本周，Microsoft 被披露存在 XML 外部实体注入漏洞。攻击者可利用该漏洞获取敏感信息，在受影响应用程序上下文中执行任意代码。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-2016-12245>

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-201	Moxa NPort5110 TCP/IP 协议栈	高	无

6-12094	存在拒绝服务漏洞		
CNVD-2016-12159	FreeBSD telnetd(8) login(1)参数注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://security.freebsd.org/advisories/FreeBSD-SA-16:36.telnetd.asc
CNVD-2016-12161	Dell SonicWALL Universal Management Suite SQL 注入漏洞	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://www.zerodayinitiative.com/advisories/ZDI-16-617/
CNVD-2016-12184	PHP 'locale_get_display_name()' 栈缓冲区溢出漏洞	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.php.net/
CNVD-2016-12203	Linux Kernel 本地权限提升漏洞（CNVD-2016-12203）	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： https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=76cc404bfcd0d419c720de4daaf2584542734f42
CNVD-2016-12218	BMC Patrol 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.bmc.com/
CNVD-2016-12385	PHP FormMail Generator 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： http://www.formmail-maker.com/generator.php
CNVD-2016-12386	PHP FormMail Generator 安全绕过漏洞（CNVD-2016-12386）	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.formmail-maker.com/generator.php
CNVD-2016-12387	PHP FormMail Generator 安全绕过漏洞（CNVD-2016-12387）	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.formmail-maker.com/generator.php

表 4 部分重要高危漏洞列表

小结：12 月 13 日，微软发布了 2016 年 12 月份的月度例行安全公告，共含 12 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Office、Office Services、.NET Framework 和 Web Apps 中存在的 41 个安全漏洞。攻击者可提升权限，远程执行任意代码。此外，Google、Adobe、Cisco 等多款产品被披露存在多个安全漏洞，攻击者利

用漏洞可执行任意代码、绕过安全限制或发起拒绝服务攻击等。另外，Microsoft 被披露存在 XML 外部实体注入漏洞。攻击者可利用该漏洞获取敏感信息，在受影响应用程序上下文中执行任意代码。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. 雅虎邮箱存储型 XSS 漏洞，黑客能看任何人的邮件

最近来自芬兰 Klikki Oy 的研究员 Jouko Pynnönen 发表了一篇博客，其中演示了恶意攻击者如何利用 XSS 漏洞攻下雅虎邮箱，将受害者收件箱中的邮件发到外部站点；以及构建病毒，这个病毒可以通过向邮件签名中添加恶意脚本，附加在所有传出的电子邮件中。由于恶意代码就位于邮件消息的正文中，代码会在受害者打开邮件时立即执行，不需要其他交互过程。所有问题的症结实际上在于雅虎邮箱无法正确过滤 HTML 邮件中潜在的恶意代码。

参考链接：<http://www.freebuf.com/vuls/122455.html>

2. McAfee VirusScan Linux 企业版存在多个高危漏洞

几个月之前，麻省理工学院林肯实验室的安全专家 Andrew Fasano 就在 McAfee VirusScan Linux 企业版（VSEL）中发现多个漏洞，这些漏洞存在于 VSEL 1.9.2 版本至 2.0.2 版本。本次公布的泄露信息中，McAfee VirusScan Linux 企业版受到各种漏洞的影响，包括信息泄露，跨站点请求伪造（CSRF），跨站点脚本（XSS），远程代码执行，特权升级，特殊元素注入，暴力枚举身份认证，SQL 注入和任意文件写入的问题。受到漏洞影响的用户应尽快升级到 Endpoint Security for Linux（ENSL）10.2 或更高版本，VSEL 产品很快就会寿终正寝。

参考链接：<http://www.freebuf.com/news/122905.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