

信息安全漏洞周报

2017 年 03 月 20 日-2017 年 03 月 26 日

2017年第13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 253 个，其中高危漏洞 85 个、中危漏洞 153 个、低危漏洞 15 个。漏洞平均分为 5.93。本周收录的漏洞中，涉及 0day 漏洞 65 个（占 26%）。本周虽然有较多 Apache Struts2 S2-046 漏洞的威胁预警及案例报告，但根据 CNVD 抽样测试，此前 Apache Struts2 S2-045 漏洞涉及党政机关和重要和行业单位的案例通报后处置修复率超过 85%，因此威胁态势整体评价未出现较大变化。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 624 个，与上周（408 个）环比增加 53%。

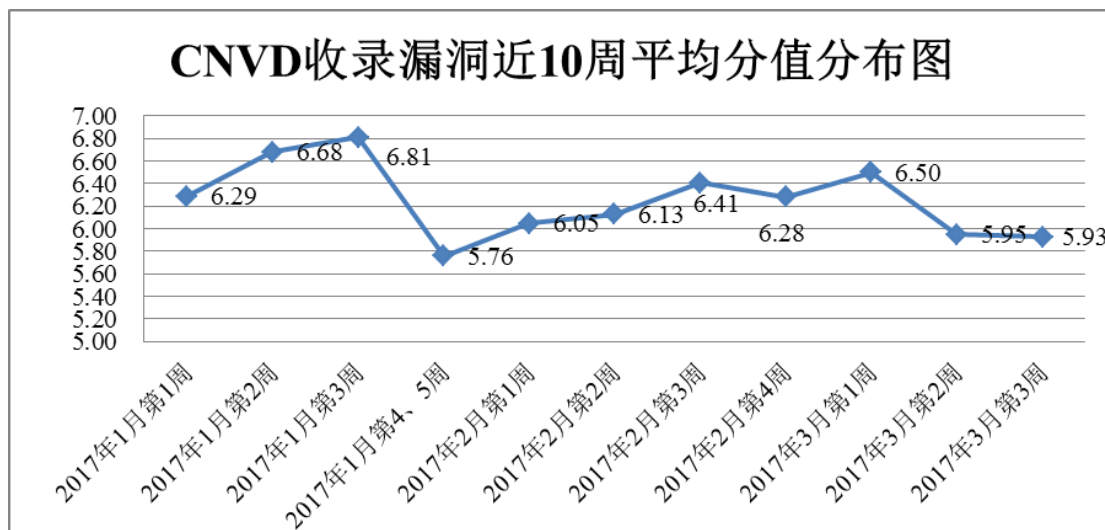


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 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 253 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、绿盟科技、华为技术有限公司、天融信等单位报送数量较多。漏洞盒子、江西安服信息产业有限公司、广西

鑫瀚科技有限公司、广州神月信息技术有限公司、上海零盾网络科技有限公司、山东安云信息技术有限公司及其他个人白帽子向 CNVD 提交了 624 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
启明星辰	198	0
安天实验室	170	0
360 网神	113	113
绿盟科技	105	0
华为技术有限公司	84	0
天融信	83	0
H3C	79	0
恒安嘉新	29	0
杭州安恒信息技术有限公司	28	0
安全狗	22	4
阿里云计算有限公司	13	0
北京数字观星科技有限公司	5	0
知道创宇	3	1
南京铨迅信息技术股份有限公司	4	4
深圳市深信服电子科技有限公司	3	3
西安四叶草信息技术有限公司	1	1
漏洞盒子	353	353
江西安服信息产业有限公司	10	10
广西鑫瀚科技有限公司	8	8
广州神月信息技术有限公司	6	6

上海零盾网络科技有限公司	1	1
山东安云信息技术有限公司	1	1
CNCERT 山西分中心	13	13
CNCERT 海南分中心	11	11
CNCERT 江西分中心	9	9
CNCERT 重庆分中心	8	8
CNCERT 广东分中心	3	3
CNCERT 河南分中心	3	3
CNCERT 湖北分中心	3	3
CNCERT 上海分中心	3	3
CNCERT 山东分中心	2	2
CNCERT 宁夏分中心	1	1
CNCERT 河北分中心	1	1
个人	62	62
报送总计	1438	624
录入总计	253（去重）	624

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 253 个漏洞。其中应用程序漏洞 125 个，web 应用漏洞 74 个，操作系统漏洞 40 个，网络设备漏洞 11 个，安全产品漏洞 2 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	125
web 应用漏洞	74
操作系统漏洞	40
网络设备漏洞	11
安全产品漏洞	2
数据库漏洞	1

表 2 漏洞按影响类型统计表

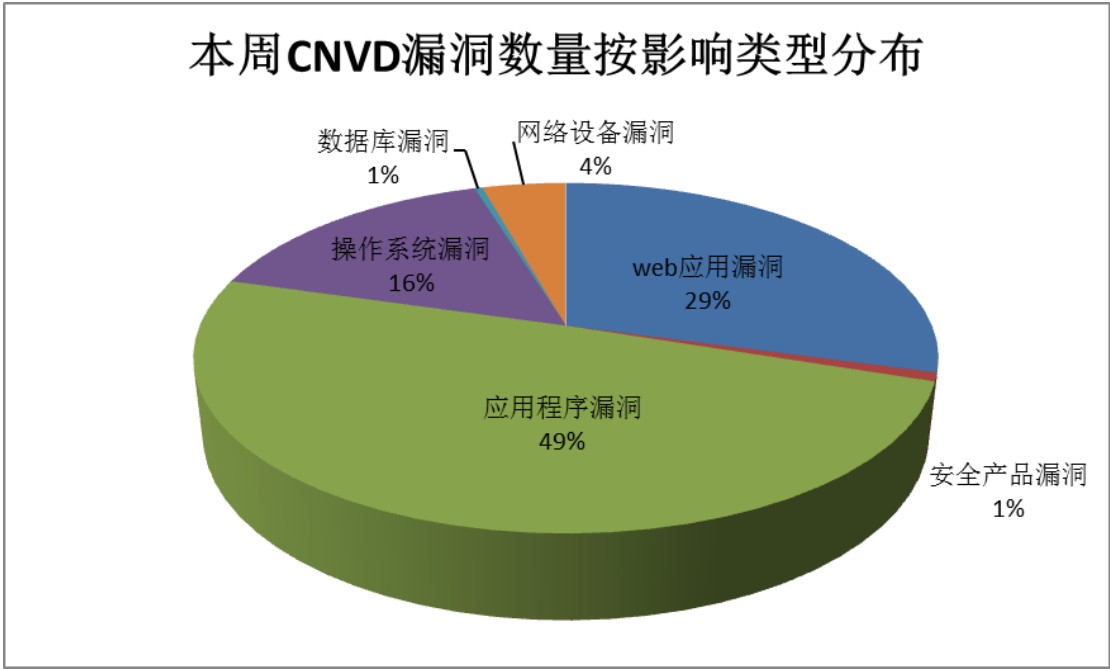


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、WordPress 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	29	11%
2	Microsoft	17	7%
3	WordPress	19	8%
4	Joomla!	15	6%
5	IBM	13	5%
6	ImageMagick	13	5%
7	WebPagetest	9	4%
8	Zoneminder	6	2%
9	Epesi	5	2%
10	其他	127	50%

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 14 个电信行业漏洞，22 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，“Cisco IOS 和 IOS XE Software 远程代码执行漏洞、

Cisco StarOS 权限提升漏洞、Google Android Audioserver 拒绝服务漏洞、Google Android Recovery Verifier 权限提升漏洞、Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-03245、CNVD-2017-03246、CNVD-2017-03247、CNVD-2017-03248）”等的综合评级为“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/>

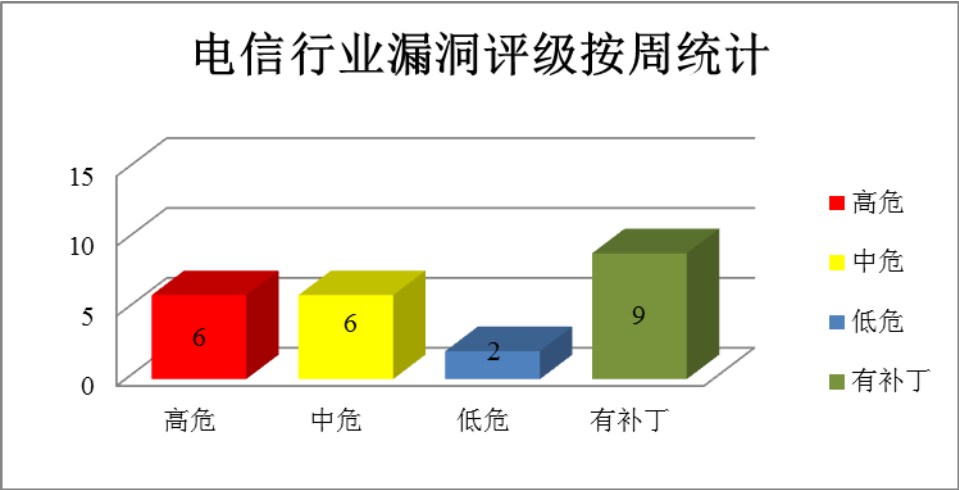


图 3 电信行业漏洞统计

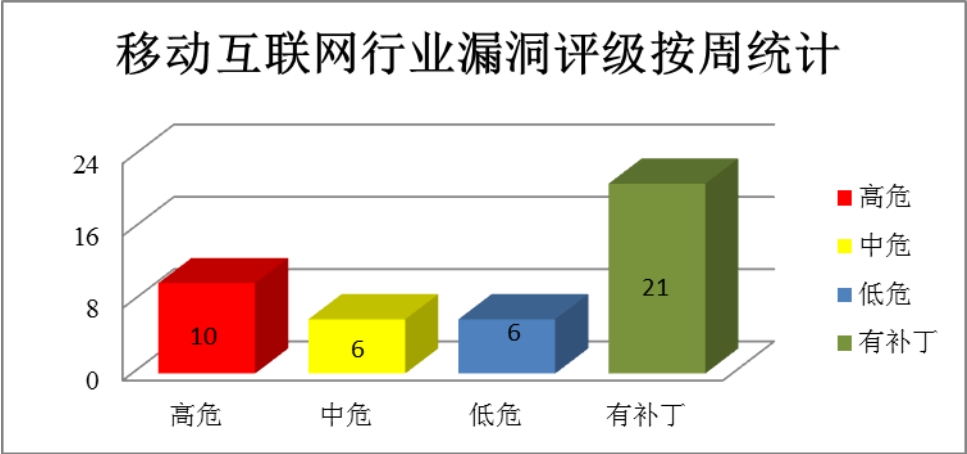


图 4 移动互联网行业漏洞统计

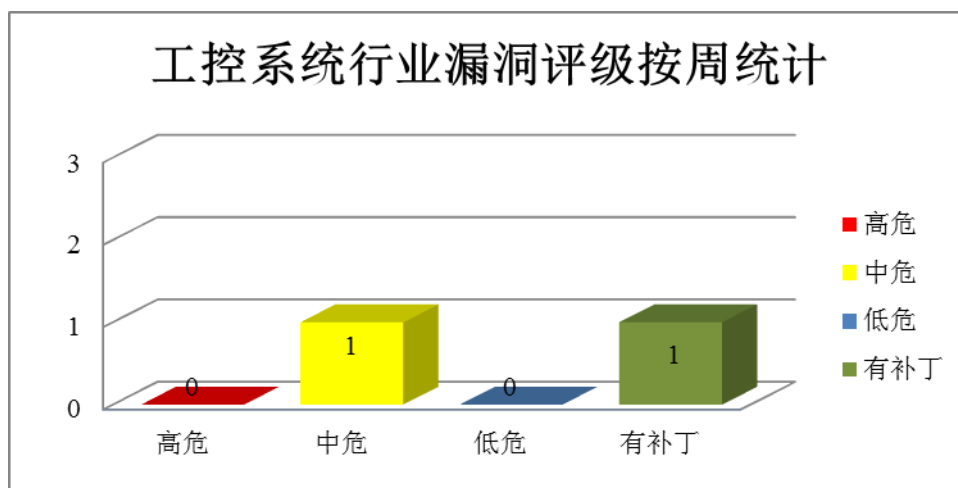


图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Mediaserver 一个提供多媒体服务的进程。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：Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-03245、CNVD-2017-03246、CNVD-2017-03247、CNVD-2017-03248、CNVD-2017-03249、CNVD-2017-03250、CNVD-2017-03251）、Google Android Audioserver 拒绝服务漏洞。上述的综合评级为“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-2017-03245>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03246>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03247>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03248>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03249>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03250>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03251>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03275>

2、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软公司发布的一系列操作系统。Uniscribe 是其中的一个能够使 Windows 操作系统正确演示 Unicode 文字的组件。Graphics Component 是其中的视窗图形组件。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执

行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Graphics Component 远程代码执行漏洞、Microsoft Windows Uniscribe 远程代码执行漏洞（CNVD-2017-03290、CNVD-2017-03291、CNVD-2017-03292、CNVD-2017-03293、CNVD-2017-03294、CNVD-2017-03295）、Microsoft Windows Uniscribe 远程代码执行漏洞。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-2017-03278>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03290>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03291>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03292>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03293>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03294>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03295>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03296>

3、IBM 产品安全漏洞

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM WebSphere MQ 一款消息传递中间件产品。IBM Tivoli Storage Manager（TSM）是一套备份和恢复管理解决方案。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、泄露敏感信息和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM SQL 注入漏洞、IBM QRadar SIEM XML 外部实体注入漏洞、IBM WebSphere MQ 拒绝服务漏洞（CNVD-2017-03082）、IBM Tivoli Storage Manager SQL 注入漏洞、IBM Tivoli Monitoring 基础服务漏洞、IBM QRadar SIEM 认证绕过漏洞、IBM QRadar SIEM 拒绝服务漏洞、IBM QRadar SIEM 信息泄漏漏洞。其中“IBM QRadar SIEM XML 外部实体注入漏洞、IBM QRadar SIEM 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-2017-03086>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03084>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03082>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03081>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03094>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03155>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03156>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03157>

4、Joomla!产品安全漏洞

Joomla!是美国 Open Source Matters 团队开发的一套开源的内容管理系统(CMS)。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞访问或修改数据库数据。

CNVD 收录的相关漏洞包括：Joomla! Spinner 360 组件 SQL 漏洞、Joomla! AJAX Search for K2 组件 SQL 注入漏洞、Joomla! Community Polls 组件 SQL 注入漏洞、Joomla! Community Surveys 组件 SQL 注入漏洞、Joomla! Community Quiz 组件 SQL 注入漏洞、Joomla! Intranet Attendance Track 组件 SQL 注入漏洞、Joomla! JO Facebook Gallery 组件 SQL 注入漏洞、Joomla! Guesser SQL 注入漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了除“Joomla! Spinner 360 组件 SQL 漏洞、Joomla! Guesser SQL 注入漏洞”以外漏洞的修补程序。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-2017-03007>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03012>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03011>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03010>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03009>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03006>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03005>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-03002>

5、ASUSWRT RT-AC53 会话窃取漏洞

ASUSWRT 是 ASUS 路由器固件。本周，ASUS 被披露存在会话窃取漏洞，远程攻击者可通过在某些 HTTP 头中发送 cgi_logout 和 asusrouter-Windows-IFTTT-1.0 来窃取任何活动的管理会话。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-2017-03113>

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-2017-02833	fastjson 远程代码执行漏洞	高	官方已经发布了版本更新，建议用户升级到最新版本，下载页面如下： http://repo1.maven.org/maven2/com/alibaba/fastjson/1.2.29/
CNVD-2017-03112	Mozilla Firefox 和 Thunderbird 内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/

CNVD-2017-03137	X.org X Server libICE 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.x.org/wiki/
CNVD-2017-03140	espeak-ruby gem 远程命令执行漏洞	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： https://github.com/dejan/espeak-ruby/issues/7
CNVD-2017-03149	Admidio SQL 注入漏洞（CNVD-2017-03149）	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://github.com/hamkovic/Admidio-3.2.5-SQLi
CNVD-2017-03165	ZoneMinder SQL 注入漏洞（CNVD-2017-03165）	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://zoneminder.com/
CNVD-2017-03166	ZoneMinder 会话固定漏洞	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://zoneminder.com/
CNVD-2017-03169	mallbuilder 前台 plugin_product_class.php 页面存在 SQL 注入漏洞	高	此产品已经下线不再出售，请关注厂商主页及时更新： http://www.mall-builder.com/
CNVD-2017-03205	Xen 'p2m'页面内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.xen.org/

表 5 部分重要高危漏洞列表

小结：本周，Google 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。此外，Microsoft、IBM、Joomla!等多款产品被披露存在多个漏洞，攻击者利用漏洞可泄露敏感信息、访问或修改数据库数据、执行任意代码或发起拒绝服务攻击等。另外，ASUS 被披露存在会话窃取漏洞，远程攻击者可通过在某些 HTTP 头中发送 `cgi_logout` 和 `asusrouter-Windows-IFTTT-1.0` 来窃取任何活动的管理会话。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. GitLab 高危漏洞可致 private token 等敏感信息泄露

GitLab 于昨日发布了 8.17.4、8.16.8 和 8.15.8 版本（社区版和企业版），修复多个高危漏洞，包含一个针对关键信息泄露漏洞的更新补丁。漏洞可导致拥有向其他用户发送 issue 或 merge 请求权限的攻击者获取到该用户的 private token, email token, email 地址

和加密的 OTP secret。想要利用漏洞需要有 Reporter 级别的权限。通过 Gitlab API 和这些敏感信息，就能以该用户权限进行操作，如果目标用户是管理员则可能产生更大危害。因此强烈建议受影响用户尽快升级。

参考链接：<http://www.freebuf.com/vuls/129906.html>

2. 思科发现其 IOS 与 IOS XE 软件集群管理协议存在远程代码执行漏洞

思科发现了存在于 IOS/IOS XE 之中的漏洞，影响范围超过 300 款不同型号的交换机，从 2350-48TD-S 交换机到 SM-X Layer 2/3 EtherSwitch 服务模块。该漏洞存在于思科 IOS 与 IOS XE 软件的 CMP 协议（思科集群管理协议）处理代码中，可被未经授权的攻击者利用，提升权限并远程执行代码，另外还能导致设备重新加载。攻击者因此也就能够获得设备的完整控制权了。思科专家暂时提供了缓解措施，就是禁用 Telnet 连接，并表示 SSH 依然是远程访问设备的最佳选择。

参考链接：<http://www.freebuf.com/vuls/129906.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