国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 07 月 17 日-2017 年 07 月 23 日　　2017 年第 30 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 309 个，其中高危漏洞 69 个、中危漏洞 208 个、低危漏洞 32 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 104 个（占 34%），其中互联网上出现“Netgear DGN2200 dnslookup.cgi 命令注入漏洞”等零日代码攻击漏洞。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 1352 个，与上周（1192 个）环比增长 13%。

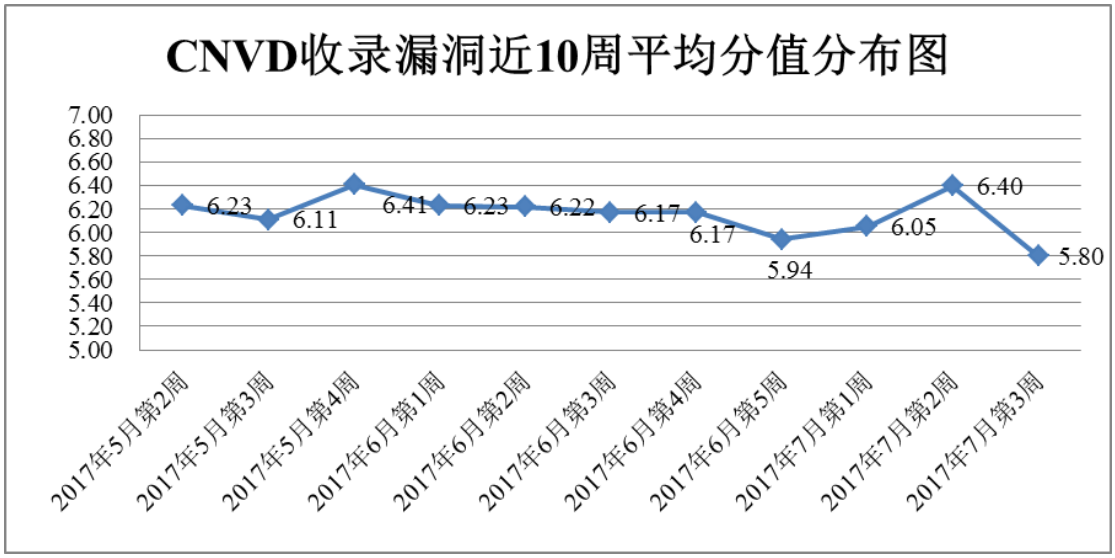

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、企业用户及个人用户报送了本周收录的全部 309 个漏洞。报送情况如表 1 所示。其中，天融信、恒安嘉新、安天实验室、H3C、华为技术有限公司等单位报送数量较多。漏洞盒子、广州神月信息安全技术有限公司、上海零盾网络科技有限公司、中新网络信息安全股份有限公司、江苏同袍信息科技有限公司、深圳鼎安

天下信息科技有限公司、中国航天科工集团第四研究院软件评测中心（北京）、南京联成科技发展股份有限公司、山石网科通信技术有限公司、清远职业技术学院、网信智安、杭州朔方信息技术有限公司、安徽新华博信息技术股份有限公司、北京安码科技有限公司、上海犇众信息技术有限公司、广州软云计算机科技有限公司、六壬网安、中电长城网际系统应用有限公司、广州万方计算机科技有限公司及其他个人白帽子向 CNVD 提交了 1352 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
漏洞盒子	235	235
天融信	202	3
恒安嘉新	170	0
安天实验室	146	0
H3C	120	2
华为技术有限公司	120	0
中国电信集团系统集成有限责任公司	97	21
启明星辰	73	0
杭州安恒信息技术有限公司	53	0
绿盟科技	50	0
北京数字观星科技有限公司	46	5
厦门服云信息科技有限公司	42	0
知道创宇	1	1
东软	1	1
南京铱迅信息技术股份有限公司	1	1
广州神月信息安全技术有限公司	21	21
上海零盾网络科技有限公司	19	19
中新网络信息安全股份有限公司	18	18

江苏同袍信息科技有限公司	14	14
深圳鼎安天下信息科技有限公司	10	10
中国航天科工集团第四研究院软件评测中心（北京）	9	9
南京联成科技发展股份有限公司	6	6
山石网科通信技术有限公司	5	5
清远职业技术学院	5	5
网信智安	5	5
杭州朔方信息技术有限公司	4	4
安徽新华博信息技术股份有限公司	3	3
北京安码科技有限公司	3	3
上海犇众信息技术有限公司	2	2
广州软云计算机科技有限公司	2	2
六壬网安	2	2
中电长城网际系统应用有限公司	2	2
广州万方计算机科技有限公司	1	1
浙江分中心	4	4
河北分中心	2	2
吉林分中心	2	2
CNCERT 广东分中心	1	1
个人	943	943
报送总计	2440	1352
录入总计	309（去重）	1352

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 309 个漏洞。其中应用程序漏洞 206 个，web 应用漏洞 57 个，操作系统漏洞 18 个，网络设备漏洞 17 个，数据库漏洞 6 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	206
web 应用漏洞	57
操作系统漏洞	18
网络设备漏洞	17
数据库漏洞	6
安全产品漏洞	5

表 2 漏洞按影响类型统计表

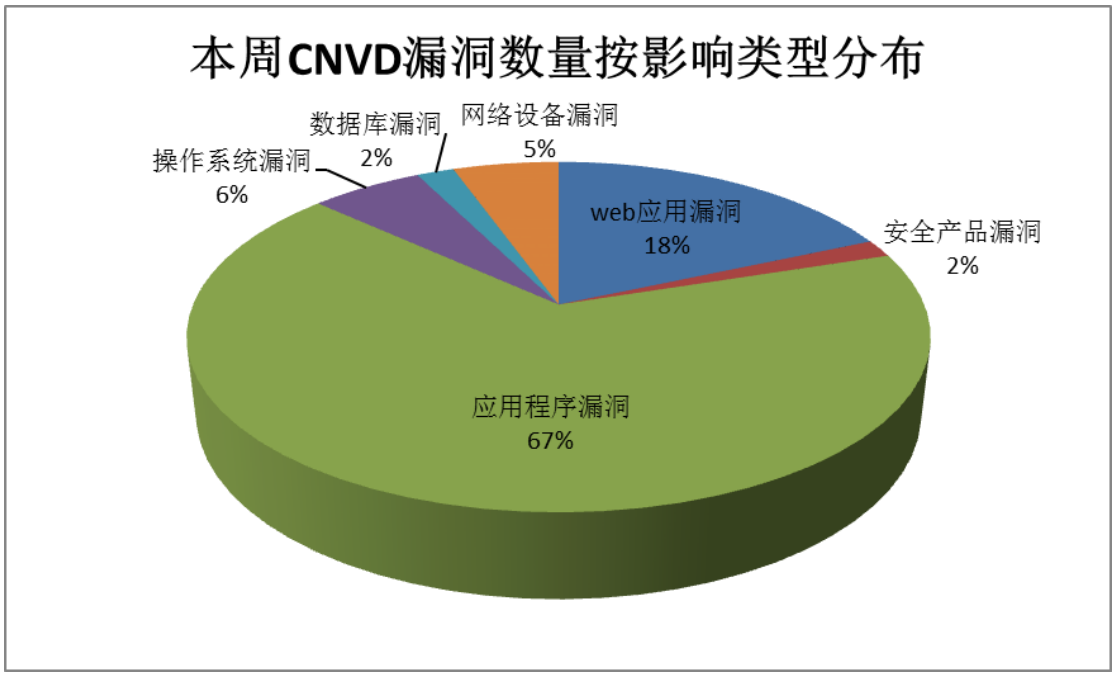

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、IBM、IrfanView 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	Oracle	25	8%
2	IBM	25	8%
3	IrfanView	24	8%
4	XnView	12	4%
5	FineCMS	11	4%

6	WordPress	10	3%
7	Microsoft	9	3%
8	SWFTools	8	3%
9	Linux	6	2%
10	其他	181	57%

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 13 个电信行业漏洞，5 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。其中，“niushop_b2c Pay.php 存在 xml 实体注入漏洞、Google Android NVIDIA Libnvparser 组件权限提升漏洞、Ecava IntegraXor SQL 注入漏洞、Rockwell Automation PanelView Plus 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/

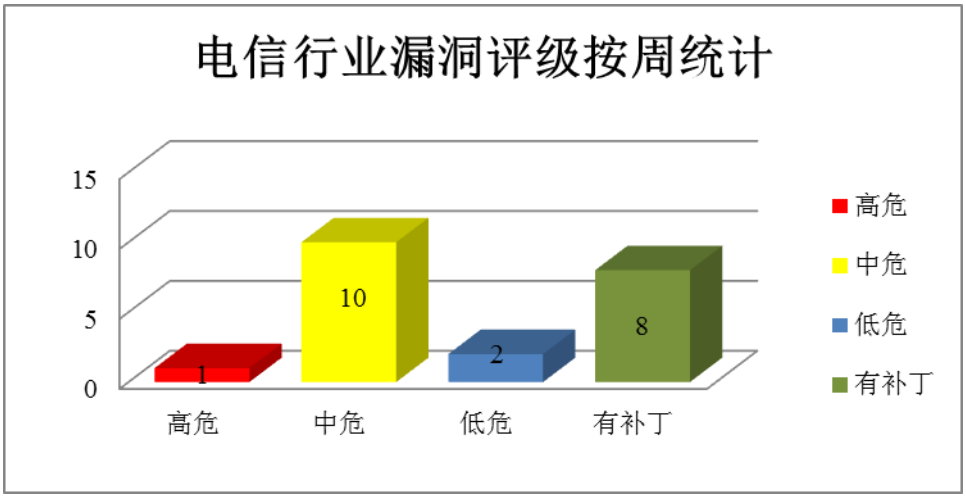

图 3 电信行业漏洞统计

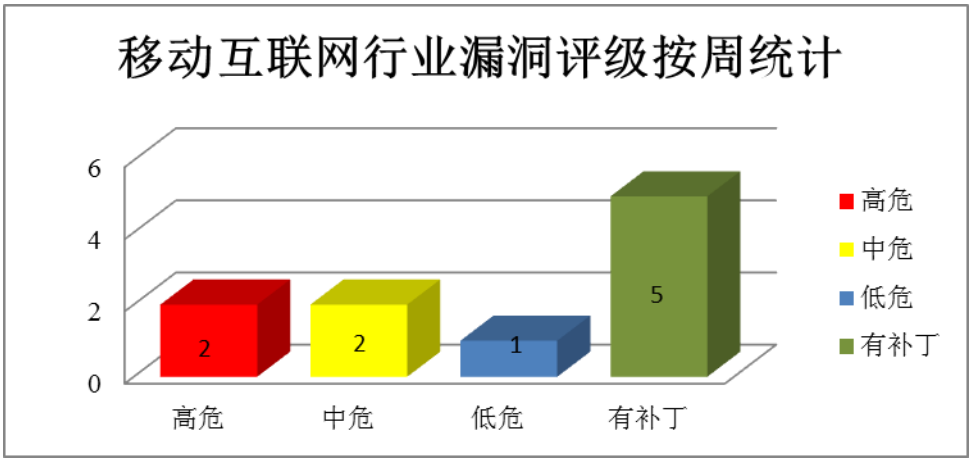

图 4 移动互联网行业漏洞统计

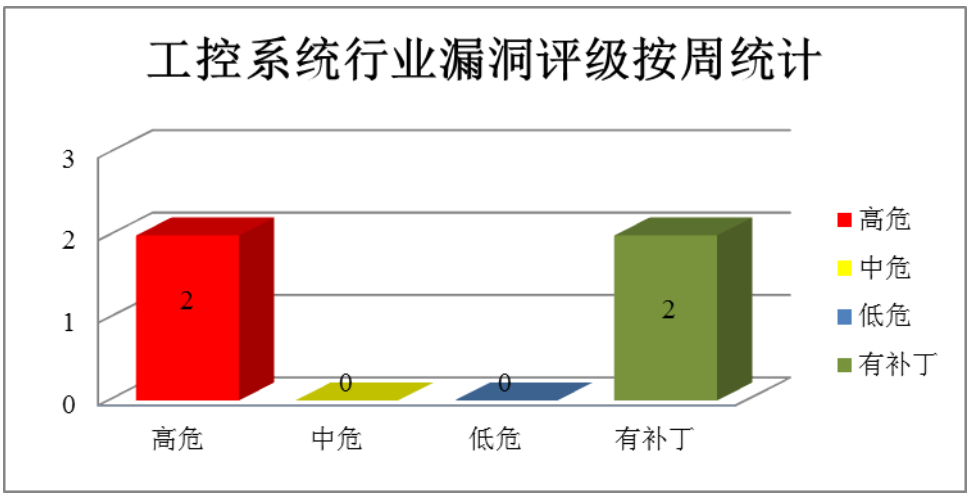

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle E-Business Suite 是美国甲骨文（Oracle）公司的一套全面集成式的全球业务管理软件。本周，该产品被披露存在未明漏洞，攻击者可利用漏洞未授权更新、插入和删除数据，影响数据的完整性。

CNVD 收录的相关漏洞包括：Oracle E-Business Suite 存在未明漏洞（CNVD-2017-15372、CNVD-2017-15373、CNVD-2017-15374、CNVD-2017-15375、CNVD-2017-15376、CNVD-2017-15377、CNVD-2017-15378、CNVD-2017-15379）。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-2017-15372

http://www.cnvd.org.cn/flaw/show/CNVD-2017-15373

http://www.cnvd.org.cn/flaw/show/CNVD-2017-15374
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15375
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15376
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15377
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15378
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15379

2、IBM 产品安全漏洞

IBM Security Guardium 是美国 IBM 公司的一套提供数据保护功能的平台。IBM DB2 Universal Database Server 是一款商业关系数据库系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露数据库敏感信息、绕过安全限制或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM DB2 缓冲区溢出漏洞（CNVD-2017-14908）、IBM Security Guardium SQL 注入漏洞、IBM Security Guardium XML 外部实体注入漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2017-15926）、IBM Security Guardium 操作系统命令注入漏洞、IBM Security Guardium 跨站脚本漏洞（CNVD-2017-15930）、IBM Security Guardium 安全绕过漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2017-15932）。其中，“IBM Security Guardium SQL 注入漏洞”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-2017-14908
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15924
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15925
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15926
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15927
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15930
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15931
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15932

3、Microsoft 产品安全漏洞

Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Skype 是一款即时通讯软件。Microsoft Malware Protection Engine 是一款微软的恶意程序保护引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码或绕过安全限制等。

CNVD 收录的相关漏洞包括：Microsoft Skype 'MSFTEDIT.DLL'缓冲区溢出漏洞、Microsoft Edge 欺骗漏洞（CNVD-2017-14641）、Microsoft Edge 安全绕过漏洞（CNVD-2017-14644）、Microsoft Edge 远程代码执行漏洞（CNVD-2017-14639）、Microsoft Edge 远程代码执行漏洞（CNVD-2017-14640）、Microsoft Edge 脚本引擎远程内存破坏漏洞

（CNVD-2017-14642）、Microsoft Edge 脚本引擎远程内存破坏漏洞（CNVD-2017-14643）、Microsoft Malware Protection Engine 远程执行代码漏洞。除“Microsoft Skype 'MSFTEDIT.DLL'缓冲区溢出漏洞、Microsoft Edge 欺骗漏洞（CNVD-2017-14641）、Microsoft Edge 安全绕过漏洞（CNVD-2017-14644）”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/flaw/show/CNVD-2017-15887
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14641
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14644
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14639
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14640
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14642
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14643
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15844

4、WordPress 产品安全漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，该产品被披露存在目录遍历、跨站脚本和 SQL 注入漏洞等，攻击者可利用漏洞泄露数据库敏感信息或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：WordPress Responsive Lightbox 插件跨站脚本漏洞、WordPress Shortcodes Ultimate 插件目录遍历漏洞、WordPress Photo Gallery 目录遍历漏洞、WordPress WP Statistics 插件跨站脚本漏洞、WordPress WP Statistics 插件 SQL 注入漏洞、WordPress All-in-One WP Migration 插件跨站脚本漏洞、WordPress How-Interest 插件跨站脚本漏洞、WordPress DSubscribers 插件 SQL 注入漏洞。其中，“WordPress DSubscribers 插件 SQL 注入漏洞、WordPress WP Statistics 插件 SQL 注入漏洞”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-2017-15110
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15111
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15388
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15389
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15390
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15391
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15392
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15393

5、NetBSD 任意代码执行漏洞

NetBSD 是一款基于 BSD 的操作系统。本周，NetBSD 被披露存在任意代码执行漏洞，攻击者可利用漏洞在受影响的系统的上下文中执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2017-15812

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-2017-15534	GNU glibc 本地内存破坏漏洞	高	用户可联系供应商获得补丁信息：http://www.gnu.org/
CNVD-2017-15538	Acronis True Image 中间人绕过安全漏洞	高	用户可联系供应商获得补丁信息：https://www.acronis.com/
CNVD-2017-15544	Linux Kernel 'offset2lib'本地安全绕过漏洞	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.kernel.org/
CNVD-2017-15807	Ecava IntegraXor SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://ics-cert.us-cert.gov/advisories/ICSA-17-171-01
CNVD-2017-15818	Trend Micro InterScan Web Security 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/1117413
CNVD-2017-15843	Linux Kernel 权限提升漏洞（CNVD-2017-15843）	高	用户可联系供应商获得补丁信息：https://www.kernel.org/
CNVD-2017-15852	Inside Secure MatrixSSL 缓冲区溢出漏洞（CNVD-2017-15852）	高	用户可联系供应商获得补丁信息：http://www.matrixssl.org/
CNVD-2017-15853	Inside Secure MatrixSSL 缓冲区溢出漏洞（CNVD-2017-15853）	高	用户可联系供应商获得补丁信息：http://www.matrixssl.org/
CNVD-2017-15890	Netgear DGN2200 dnslookup.cgi 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://kb.netgear.com/
CNVD-2017-15913	多款 Newport 产品认证绕过漏洞	高	用户可联系供应商获得补丁信息：https://www.newport.com/

表 4 部分重要高危漏洞列表

小结：本周，Oracle 被披露存在未明漏洞，攻击者可利用漏洞未授权更新、插入和删除数据，影响数据的完整性。此外，IBM、Microsoft、WordPress 等多款产品被披露存在多个漏洞，攻击者利用漏洞可泄露数据库敏感信息、绕过安全限制或进行跨站脚本攻击等。另外，NetBSD 被披露存在任意代码执行漏洞，攻击者可利用漏洞在受影响的系统的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. gSOAP 开源软件开发库曝“绿萝”漏洞，数百万 IoT 设备岌岌可危

IoT 安全公司 Senrio 的研究员最先在 gSOAP 中发现这个漏洞（编号 CVE-2017-9765 ），并将其命名为 “Devil’s Ivy”（绿萝）。“绿萝” 是一个堆栈缓冲区溢出漏洞，可允许黑客远程攻击（DOS 攻击） SOAP Web 服务后台程序，并在存在漏洞的设备上执行任意代码，可能会影响数百万 IoT 设备。

参考链接：http://www.freebuf.com/news/140878.html

2. 思科 WebEx 视频会议插件再度发现严重 RCE 漏洞

思科的 WebEx 浏览器插件（Chrome 和 Firefox）中再度发现严重（Critical）远程执行代码漏洞（CVE-2017-6753），这已经是今年第二次在 WebEx 中发现严重漏洞。攻击者可利用该漏洞在目标计算机的浏览器上远程注入恶意代码，目前思科已经在 WebEx 的 1.0.12 版本中修复了这个问题。

参考链接：http://www.freebuf.com/news/140760.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