国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 3 月 5 日-2018 年 3 月 11 日 **2018 年第 10 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 386 个，其中高危漏洞 124 个、中危漏洞 228 个、低危漏洞 34 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 132 个（占 34%），其中互联网上出现“AVTECH 多个产品远程命令执行漏洞、Joomla! PrayerCenter SQL 注入漏洞”等零日代码攻击漏洞。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 641 个，与上周（679 个）环比下降 8%。

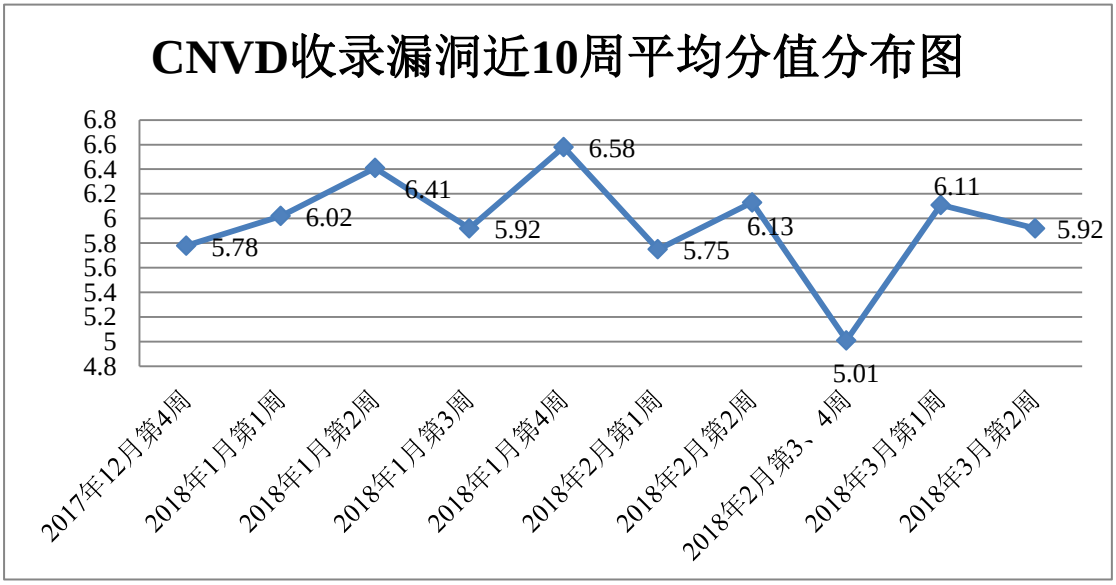

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、华为技术有限公司、哈尔滨安天科技股份有限公司、恒安嘉新(北京)科技股份公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。四川虹微技术有限公司（子午攻防实验室）、

上海观安信息技术股份有限公司、南京联成科技发展股份有限公司、福建省海峡信息技术有限公司、南瑞集团公司（国网电力科学研究院）、中新网络信息安全股份有限公司、安徽三实信息技术服务有限公司、中国信息安全测评中心华中测评中心(湖南省信息安全测评中心)、北京长亭科技有限公司、漏斗社区、北京智游网安科技有限公司、常州瑞新网络科技股份有限公司及其他个人白帽子向 CNVD 提交了 641 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 291 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
北京天融信网络安全技术有限公司	238	1
360 网神（补天平台）	167	167
华为技术有限公司	166	2
哈尔滨安天科技股份有限公司	150	0
恒安嘉新(北京)科技股份公司	111	0
新华三技术有限公司	102	0
漏洞盒子	124	124
北京数字观星科技有限公司	67	0
北京神州绿盟科技有限公司	52	0
中国电信集团系统集成有限责任公司	32	0
北京启明星辰信息安全技术有限公司	10	10
北京无声信息技术有限公司	6	0
知道创宇	2	0
杭州安恒信息技术有限公司	2	2
厦门服云信息科技有限公司	1	1
四川虹微技术有限公司（子午攻防实验室）	57	57

上海观安信息技术股份有限公司	21	21
南京联成科技发展股份有限公司	20	20
福建省海峡信息技术有限公司	17	17
南瑞集团公司（国网电力科学研究院）	12	12
中新网络信息安全股份有限公司	12	12
安徽三实信息技术服务有限公司	9	9
中国信息安全测评中心华中测评中心(湖南省信息安全测评中心)	4	4
北京长亭科技有限公司	3	3
漏斗社区	3	3
北京智游网安科技有限公司	2	2
常州瑞新网络科技股份有限公司	1	1
吉林分中心	8	8
河北分中心	2	2
CNCERT 广东分中心	1	1
西藏分中心	1	1
甘肃分中心	1	1
贵州分中心	1	1
宁夏分中心	1	1
湖南分中心	1	1
个人	157	157
报送总计	1541	641

本周漏洞按类型和厂商统计

本周，CNVD 收录了 386 个漏洞。其中应用程序漏洞 239 个，WEB 应用漏洞 89 个，操作系统漏洞 18 个，网络设备漏洞 35 个，安全产品漏洞 5 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	239
WEB 应用漏洞	89
操作系统漏洞	18
网络设备漏洞	35
安全产品漏洞	5

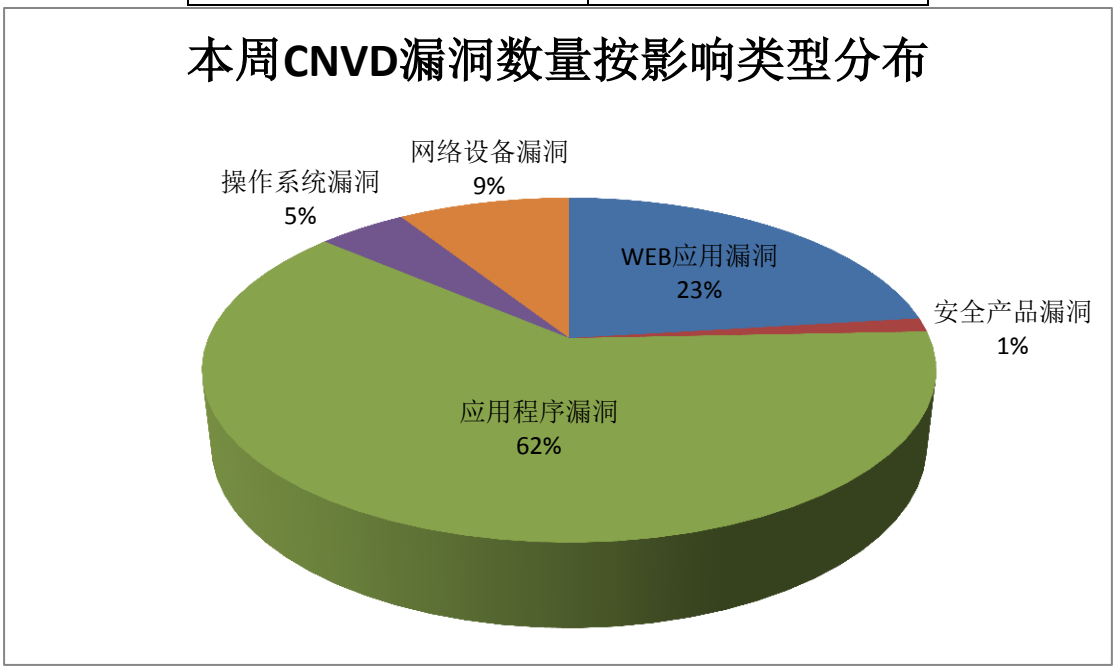

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Trend Micro、CloudBees、Gemalto 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Trend Micro	12	3%
2	CloudBees	11	3%
3	Gemalto	10	3%
4	Joomla!	10	3%
5	Google	7	2%
6	ImageMagick	6	2%
7	Atlassian	6	2%

8	WordPress	5	1%
9	F5	5	1%
10	其他	314	80%

本周行业漏洞收录情况

本周，CNVD 收录了 244 个电信行业漏洞，16 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“ASUSWRT 设备未认证修改配置漏洞、Google Android Qualcomm WLAN 整数溢出漏洞、ISC BIND 远程拒绝服务漏洞（CNVD-2018-04350）、Eaton ELCSoft 任意代码执行漏洞、Siemens 多个产品存在未授权操作漏洞”等漏洞的综合评级为“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/

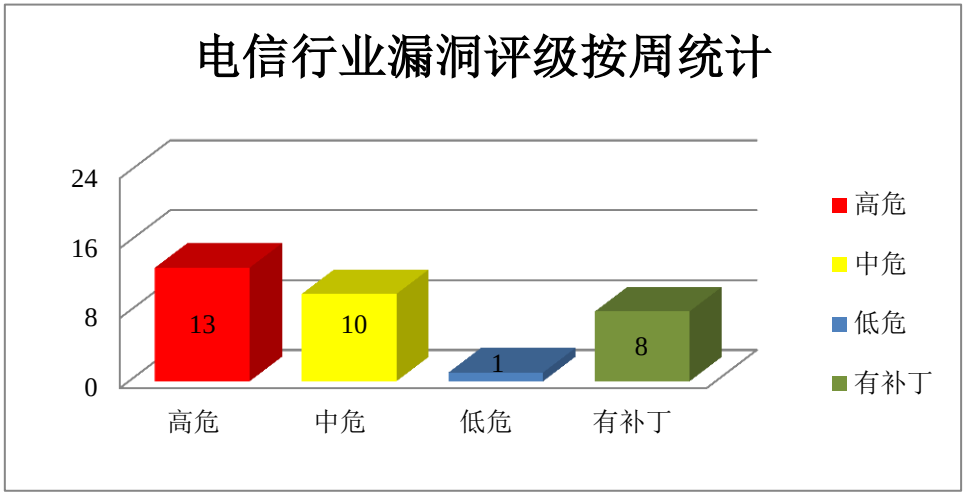

图 3 电信行业漏洞统计

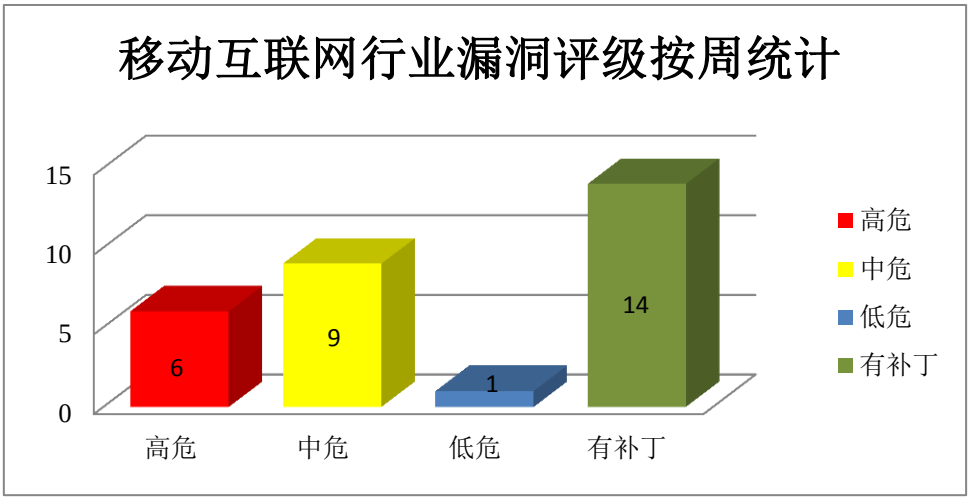

图 4 移动互联网行业漏洞统计

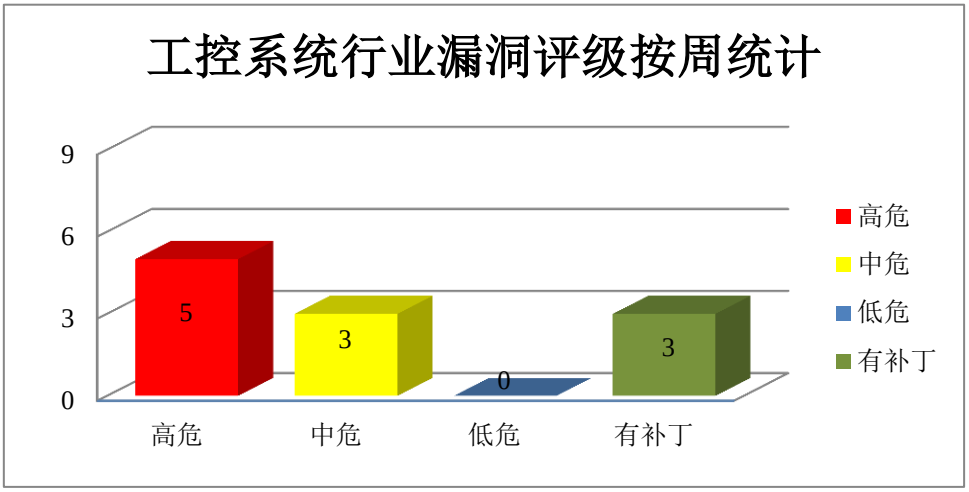

图 5 工控行业漏洞统计

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、Exim SMTP Mail Server 存在缓冲区溢出漏洞

Exim 是一个 MTA（Mail Transfer Agent，邮件传输代理）服务器软件。本周，该产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Exim SMTP Mail Server 缓冲区溢出漏洞。该漏洞的综合评级为“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-2018-04619

2、Google 产品安全漏洞

Android on Google Pixel 和 Nexus 是美国谷歌的一套运行于 Google Pixel 和 Nexus 中并以 Linux 为基础的开源操作系统。Media framework 是其中的一个多媒体开发框架。Qualcomm WLAN 是一个美国高通（Qualcomm）公司开发的无线局域网组件。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敏感信息、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Qualcomm WLAN 整数溢出漏洞、Google Android Media framework 存在未明漏洞、Google Android Media framework 拒绝服务漏洞（CNVD-2018-04666）、Google Android Media framework 远程代码执行漏洞（CNVD-2018-04665）、Google Android Qualcomm WLAN 缓冲区溢出漏洞、Google Android Qualcomm WLAN 权限提升漏洞（CNVD-2018-04763）、Google Android Media framework（libstagefright_soft_avcenc）信息泄露漏洞。除“Google Android Qualcomm WLAN 缓冲区溢出漏洞、Google Android Qualcomm WLAN 权限提升漏洞（CNV

D-2018-04763）、Google Android Media framework（libstagefright_soft_avcenc）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/flaw/show/CNVD-2018-04753

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04667

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04666

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04665

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04752

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04763

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04668

3、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、任意文件上传或跨站脚本漏洞，攻击者可利用漏上传任意文件或发起跨站脚本攻击。

CNVD 收录的相关漏洞包括：Joomla! CP Event Calendar SQL 注入漏洞、Joomla! PrayerCenter SQL 注入漏洞、Joomla! Proclaim 任意文件上传漏洞、Joomla! SQL 注入漏洞（CNVD-2018-04206）、Joomla! Visual Calendar SQL 注入漏洞、Joomla!跨站脚本漏洞（CNVD-2018-04201、CNVD-2018-04204、CNVD-2018-04205）。除“Joomla!跨站脚本漏洞（CNVD-2018-04201、CNVD-2018-04204、CNVD-2018-04205）”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-2018-04615

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04777

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04776

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04206

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04509

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04201

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04204

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04205

4、Trend Micro 产品安全漏洞

Trend Micro Email Encryption 是美国趋势科技的一套基于身份的具有电子邮件加密功能的解决方案。Trend Micro Email Encryption Gateway 是其中的一个提供数据保护的网关产品。本周，上述产品被披露存在 SQL 注入、任意命令执行和跨站脚本漏洞，攻击者可利用漏洞执行任意命令或发起跨站脚本攻击。

CNVD 收录的相关漏洞包括：Trend Micro Email Encryption Gateway SQL 注入漏

洞、Trend Micro Email Encryption Gateway SQL 注入漏洞（CNVD-2018-04493、CNVD-2018-04494）、Trend Micro Email Encryption Gateway XML 外部实体注入漏洞、Trend Micro Email Encryption Gateway 任意命令执行漏洞、Trend Micro Email Encryption Gateway 任意命令执行漏洞（CNVD-2018-04486）、Trend Micro Email Encryption Gateway 跨站脚本漏洞、Trend Micro Email Encryption Gateway 跨站脚本漏洞（CNVD-2018-04491）。除“Trend Micro Email Encryption Gateway 跨站脚本漏洞、Trend Micro Email Encryption Gateway 跨站脚本漏洞（CNVD-2018-04491）”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-2018-04492

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04493

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04494

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04489

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04490

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04491

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04484

http://www.cnvd.org.cn/flaw/show/CNVD-2018-04486

5、Dasan GPON ONT WiFi Router 缓冲区溢出漏洞

Dasan GPON ONT WiFi Router 是韩国 DASAN Networks 公司的一款无线路由器设备。本周，DASAN 被披露存在缓冲区溢出漏洞，远程攻击者可通过向/cgi-bin/login_action.cgi 文件中的‘login_action’函数发送较长的 POST 请求利用该漏洞执行任意代码。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-2018-04394

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

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-04318	Commvault 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.securifera.com/advisories/sec-2017-0001/
CNVD-2018-04350	ISC BIND 远程拒绝服务漏洞（CNVD-2018-04350）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.isc.org/article/AA-01542
CNVD-2018-04359	AsusWRT router/httpd/httpd.c 文件访问绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://blogs.securiteam.com/index.php/

			archives/3589
CNVD-2018-04360	ASUSWRT 设备未认证修改配置漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://blogs.securiteam.com/index.php/archives/3589
CNVD-2018-04363	多款 Lenovo 产品 Fingerprint Manager Pro 硬编码密码	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.lenovo.com/us/zh/product_security/len-15999
CNVD-2018-04520	小米路由器 R3D 存在远程任意命令执行漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.mi.com/
CNVD-2018-04707	Haystack Arq for Mac 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.arqbackup.com/download/
CNVD-2018-04713	epg search result viewer 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://dbit.web.fc2.com/
CNVD-2018-04714	GNU C Library 'memalign'函数整数溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://sourceware.org/bugzilla/show_bug.cgi?id=22343
CNVD-2018-04725	Haystack Arq for Mac 本地权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.arqbackup.com/download/

小结：本周，Exim 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码此外，Trend Micro、Google、Joomla!等多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、执行任意代码或提升权限等。另外，DASAN 被披露存在缓冲区溢出漏洞，远程攻击者可通过向/cgi-bin/login_action.cgi 文件中的‘login_action’函数发送较长的 POST 请求利用该漏洞执行任意代码。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. Exim 最新漏洞影响全球过半邮件服务器

中国台湾地区安全研究人员 Meh Chang 在开源邮件代理 Exim 中发现缓冲区溢出漏洞，该漏洞影响了全球过半的电邮服务器。漏洞 CVE-2018-678 被归为“预授权远程代码执行漏洞”，这就意味着，服务器验证攻击者之前，攻击者可诱骗 Exim 电邮服务器运行恶意命令。

参考链接：https://www.easyaq.com/news/1675314846.shtml

2. Memcached DDoS 攻击

当安全公司 Cloudflare 在上周报告在实际攻击活动中监测了到这种攻击时，基于 Memcached 服务器发起的 DDoS 攻击就已经开始得到了公众的关注。随着 PoC 代码的发布，情况必将会变得更糟。任何人都可以以此发起大规模的 DDoS 攻击，这种情况会一直持续到最后一台易受攻击的 Memcached 服务器被修补，或者在 11211 端口受到防火墙限制，甚至完全离线时，才能够受到控制。为了缓解普遍存在的 DDoS 攻击或者防止 Memcached 服务器被滥用作为攻击媒介。最好的选择是将 Memcached 服务器绑定到本地接口，或者完全禁用 UDP 支持（如果不使用的话）。

参考链接：https://www.hackeye.net/threatintelligence/12548.aspx

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：010-82991537