国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 05 月 08 日-2017 年 05 月 14 日 **2017 年第 20 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**高**。

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 261 个，其中高危漏洞 105 个、中危漏洞 135 个、低危漏洞 21 个。漏洞平均分值为 6.23。本周收录的漏洞中，涉及 0day 漏洞 49 个（占 19%），其中互联网上出现“Gemalto SmartDiag Diagnosis Tool 缓冲区溢出漏洞”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 842 个，与上周（617）环比增长 36%。本周末，互联网上爆发了勒索软件利用 Windows SMB 服务漏洞（MS17-010）进行大规模攻击和传播的情况，导致各部门、各行业单位和个人用户处于严重威胁。

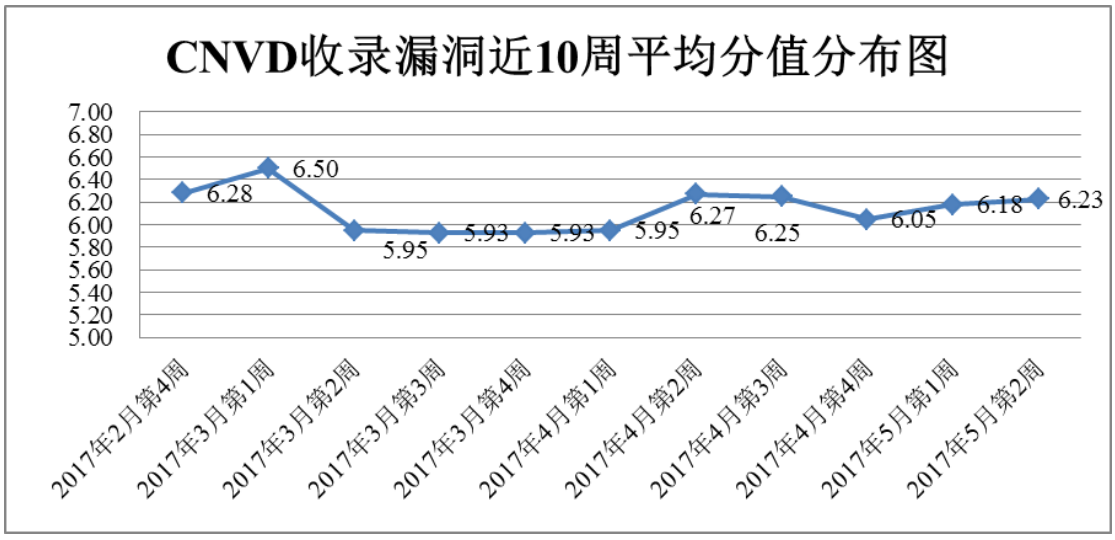

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 10 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 29 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 280 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 188

起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 21 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

北京法宣在线科技有限公司、中铁建商务管理有限公司、广州红帆电脑科技有限公司、金山软件股份有限公司、北京外研在线教育科技有限公司、华为技术有限公司、上海卓越睿新数码科技有限公司、TWhite Shark System、Advantech Co., Ltd.、枣阳市山水数码工作室、中国科学技术协会。

本周，CNVD 发布了《关于 Intel AMT 远程权限提升漏洞的安全公告》、《关于 Microsoft Malware Protection Engine 存在远程代码执行漏洞的安全公告》、《关于重点防范 Windows 操作系统勒索软件攻击的情况公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4137

http://www.cnvd.org.cn/webinfo/show/4138

http://www.cnvd.org.cn/webinfo/show/4139

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 261 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、H3C 等单位报送数量较多。福建六壬网安股份有限公司、安徽新华博信息技术股份有限公司、上海观安信息技术有限公司、河北网信智安信息技术有限公司、杭州朔方信息技术有限公司、江苏君立华域信息安全技术有限公司、北京安码科技有限公司、西安电子科技大学、上海犇众信息技术有限公司、山石网科通信技术有限公司及其他个人白帽子向 CNVD 提交了 842 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	494	494
启明星辰	142	9
安天实验室	135	0
天融信	100	0
H3C	79	0
华为技术有限公司	56	0

绿盟科技	52	0
杭州安恒信息技术有限公司	46	0
中国电信集团系统集成有限责任公司	38	0
恒安嘉新	34	1
厦门服云信息科技有限公司	23	1
北京数字观星科技有限公司	10	0
广西鑫瀚科技有限公司	5	5
北京无声信息技术有限公司	1	0
西安四叶草信息技术有限公司	1	1
南京铱迅信息技术股份有限公司	1	1
漏洞盒子	135	135
福建六壬网安股份有限公司	12	12
安徽新华博信息技术股份有限公司	5	5
上海观安信息技术有限公司	3	3
河北网信智安信息技术有限公司	3	3
杭州朔方信息技术有限公司	2	2
江苏君立华域信息安全技术有限公司	1	1
北京安码科技有限公司	1	1
西安电子科技大学	1	1
上海犇众信息技术有限公司	1	1
山石网科通信技术有限公司	1	1
CNCERT 江西分中心	12	12

CNCERT 浙江分中心	5	5
CNCERT 甘肃分中心	5	5
CNCERT 新疆分中心	3	3
CNCERT 陕西分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 上海分中心	1	1
个人	131	131
报送总计	1547	842
录入总计	261（去重）	842

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 261 个漏洞。其中应用程序漏洞 163 个， web 应用漏洞 47 个，数据库漏洞 21 个，网络设备漏洞 17 个，操作系统漏洞 12 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	163
web 应用漏洞	47
数据库漏洞	21
网络设备漏洞	17
操作系统漏洞	12
安全产品漏洞	1

表 2 漏洞按影响类型统计表

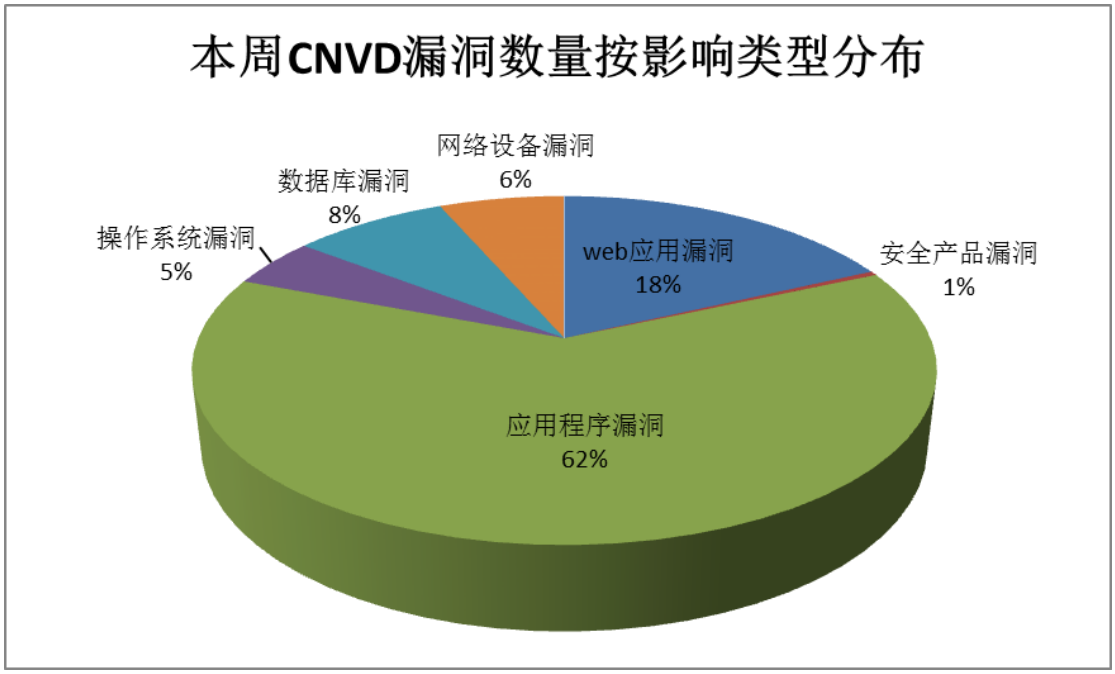

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Adobe、ImageMagick 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	78	30%
2	Adobe	9	3%
3	ImageMagick	8	3%
4	Cisco	5	2%
5	F5	5	2%
6	Juniper Networks	5	2%
7	flatCore	4	2%
8	Apache	4	2%
9	IBM	4	2%
10	其他	139	53%

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 31 个电信行业漏洞，9 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Siemens SIMATIC WinCC 和 SIMATIC WinCC Runtime Professional 拒绝服务漏洞、Youdiancms 企业网站管理系统存在反射型 XSS 跨站脚

本漏洞、Android Qualcomm sound 驱动程序权限提升漏洞（CNVD-2017-06114、CNVD-2017-06115）、Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2017-06093、CNVD-2017-06094、CNVD-2017-06095、CNVD-2017-06096）”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/

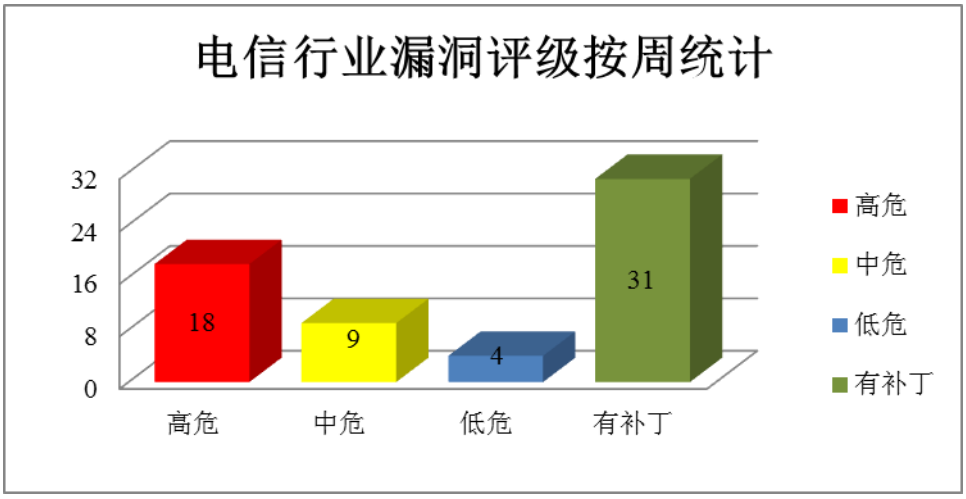

图 3 电信行业漏洞统计

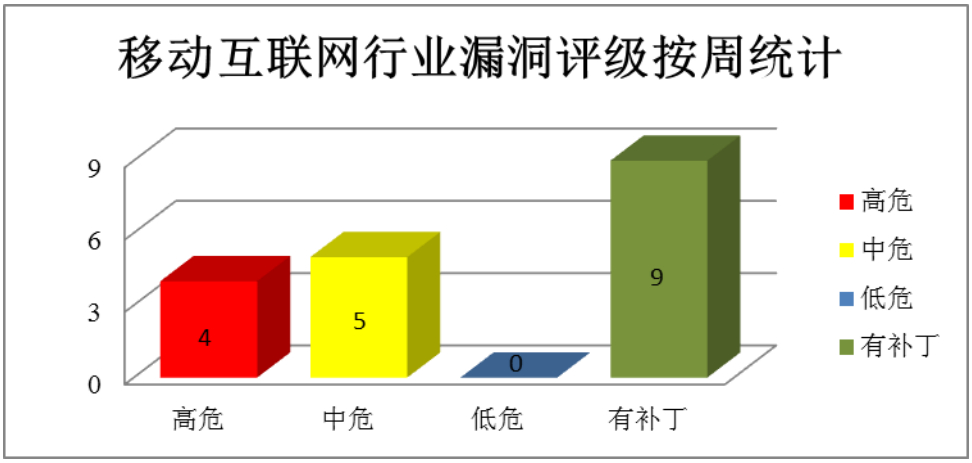

图 4 移动互联网行业漏洞统计

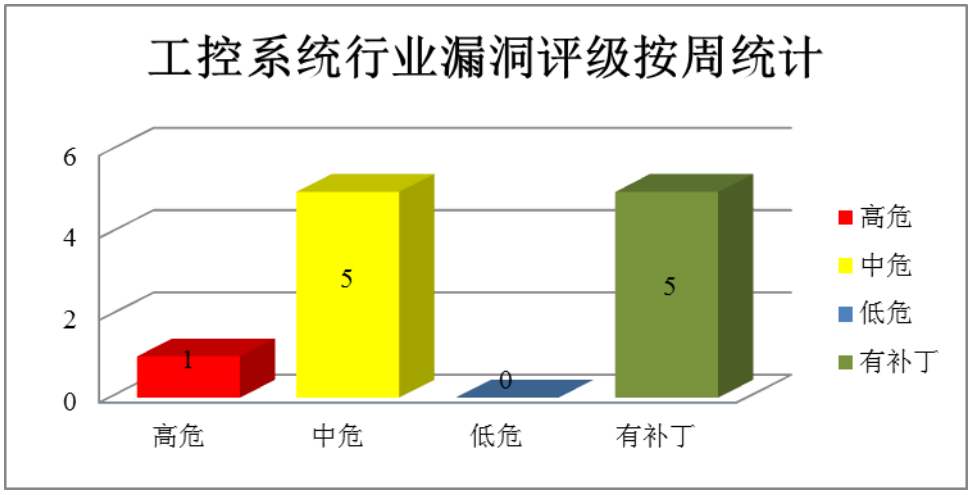

图 5 工控系统行业漏洞统计

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、Microsoft Malware Protection Engine 存在远程代码执行漏洞

Microsoft 恶意软件保护引擎（mpengine.dll）可为防病毒和反间谍软件客户端提供扫描、监测和清除功能。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞影响执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Malware Protection Engine 存在远程代码执行漏洞。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-2017-06157

2、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server component 是其中的服务器组件。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：Oracle MySQL Server 拒绝服务漏洞（CNVD-2017-06390、CNVD-2017-06391、CNVD-2017-06392、CNVD-2017-06393、CNVD-2017-06394、CNVD-2017-06397、CNVD-2017-06398、CNVD-2017-06399）。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-2017-06390

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06391

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06392

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06393

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06394

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06397

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06398

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06399

3、Adobe 产品安全漏洞

Adobe Flash Player 是美国 Adobe 公司开发的一款多媒体程序播放器，Adobe ColdFusion 是一款动态 Web 服务器产品。本周，上述产品被披露存在代码执行和 java 反序列化漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Adobe Flash Player 代码执行漏洞（CNVD-2017-06316、CNVD-2017-06317、CNVD-2017-06318、CNVD-2017-06319、CNVD-2017-06320、CNVD-2017-06321、CNVD-2017-06322）、Adobe ColdFusion java 反序列化漏洞。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-2017-06316

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06317

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06318

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06319

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06320

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06321

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06322

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06457

4、Cisco 产品安全漏洞

Cisco IOS 和 IOS XE 都是美国思科（Cisco）公司为其网络设备开发的操作系统。EnergyWise 是其中的一个能源管理架构模块。Cisco WebEx 是浏览器扩展插件。本周，上述产品被披露存在拒绝服务和信息泄露漏洞，攻击者可利用漏洞泄露敏感信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2017-06093、CNVD-2017-06094、CNVD-2017-06095、CNVD-2017-06096）、Cisco WebEx 会议服务器信息泄露漏洞。除“Cisco WebEx 会议服务器信息泄露漏洞”外，剩余漏洞的综合评级为“高危”。目前，厂商已经发布了除“Cisco WebEx 会议服务器信息泄露漏洞”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-2017-06093

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06094

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06095

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06096

http://www.cnvd.org.cn/flaw/show/CNVD-2017-06416

5、Wireless IP Camera (P2P) WIFICAM 信息泄露漏洞

Wireless IP Camera (P2P) WIFICAM 是一款远程网络摄像机。本周，Wireless IP Camera (P2P) WIFICAM 被披露存在信息泄露漏洞，攻击者可利用该漏洞借助 tcp/av0_1 or tcp/av0_0 未授权查看流量。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-2017-06440

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-2017-06154	Siemens SIMATIC WinCC 和 SIMATIC WinCC Runtime Professional 拒绝服务漏洞	高	用户可联系供应商获得补丁信息：https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-156872.pdf
CNVD-2017-06155	Smart related articles 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://gist.github.com/anonymous/14576258b0e66bb25ca4b7ca1638e51f
CNVD-2017-06224	Cygwin 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://cygwin.com/ml/cygwin/2016-02/msg00129.html
CNVD-2017-06240	Nessus 本地权限提升漏洞（CNVD-2017-06240）	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://www.tenable.com/security/tns-2017-10
CNVD-2017-06242	Mozilla Firefox 内存错误引用漏洞（CNVD-2017-06242）	高	用户可联系供应商获得补丁信息：https://www.mozilla.com/
CNVD-2017-06375	F5 BIG-IP iControl REST 远程权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://support.f5.com/csp/article/K41107914
CNVD-2017-06380	I, Librarian PDF Manager 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://i-librarian.net/article.php?id=9
CNVD-2017-06419	RIOT 栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/RIOT-OS/RIOT/pull/6961

CNVD-2017-06445	Debian inspircd package 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=780880
CNVD-2017-06447	Mozilla Network Security Services 拒绝服务漏洞	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.mozilla.com/

表 4 部分重要高危漏洞列表

小结：本周，Microsoft Malware Protection Engine 被披露存在远程代码执行漏洞，攻击者可利用漏洞影响执行任意代码。此外，Oracle、Adobe、Cisco 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、泄露敏感信息或发起拒绝服务攻击等。另外，Wireless IP Camera (P2P) WIFICAM 被披露存在信息泄露漏洞，攻击者可利用该漏洞借助 tcp/av0_1 or tcp/av0_0 未授权查看流量。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. Windows 系统恶意软件防护引擎曝严重远程代码执行漏洞

微软发布了一个安全公告——微软自家的恶意程序防护引擎出现高危安全漏洞。影响到包括 MSE、Windows Defender 防火墙等在内的产品，危害性还是相当严重的。微软恶意程序防护引擎（Microsoft Malware Protection Engine）检测某个恶意构造的文件后，攻击者就能利用漏洞实现远程代码执行。成功利用该漏洞，攻击者就能在 LocalSystem 帐号安全上下文执行任意代码，并控制系统。攻击者随后就能安装程序；查看、更改或删除数据；或者以完整的用户权限来构建新账户。。

参考链接：http://www.freebuf.com/vuls/134172.html

2. Wannacry 蠕虫勒索软件袭击全球

月 12 日晚，一款名为 Wannacry 的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索交费活动，影响到近百个国家上千家企业及公共组织。 该软件被认为是一种蠕虫变种（也被称为“Wannadecrypt0r”、“wannacryptor”或“ wcry”）。 像其他勒索软件的变种一样，WannaCry 也阻止用户访问计算机或文件，要求用户需付费解锁。

参考链接：http://www.freebuf.com/news/134512.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