国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 7 月 9 日-2018 年 7 月 15 日 **2018 年第 28 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 257 个，其中高危漏洞 76 个、中危漏洞 176 个、低危漏洞 5 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 101 个（占 39%），其中互联网上出现“Dicoogle PACS 文件包含漏洞、WordPress file-away 插件文件泄露漏洞”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 456 个，与上周（283 个）环比增长 61%。

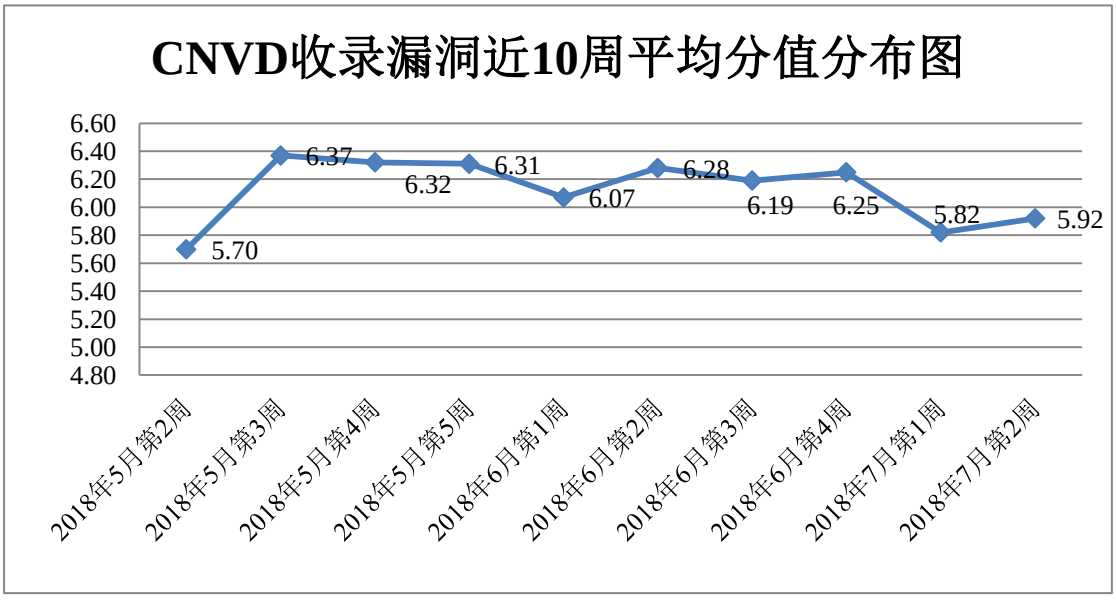

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、北京天融信网络安全技术有限公司、沈阳东软系统集成工程有限公司、哈尔滨安天科技股份有限公司、阿里云计算

有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、中新网络信息安全股份有限公司、南京联成科技发展股份有限公司、上海银基信息安全技术股份有限公司、四川虹微技术有限公司（子午攻防实验室）、任子行网络技术股份有限公司、福建省海峡信息技术公司、北京明朝万达科技股份有限公司（安元实验室）及其他个人白帽子向 CNVD 提交了 456 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 230 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
华为技术有限公司	541	0
北京天融信网络安全技术有限公司	342	7
沈阳东软系统集成工程有限公司	326	0
哈尔滨安天科技股份有限公司	265	0
阿里云计算有限公司	209	0
360 网神（补天平台）	159	159
新华三技术有限公司	106	0
北京数字观星科技有限公司	79	0
杭州安恒信息技术有限公司	74	0
漏洞盒子	71	71
北京神州绿盟科技有限公司	69	0
深圳市深信服电子科技有限公司	65	0
恒安嘉新(北京)科技股份公司	50	0
北京无声信息技术有限公司	39	0
厦门服云信息科技有限公司	6	0
北京知道创宇信息技术有限公司	2	1
山东云天安全技术有限公司	113	113

中新网络信息安全股份有限公司	11	11
南京联成科技发展股份有限公司	9	9
上海银基信息安全技术股份有限公司	9	9
四川虹微技术有限公司（子午攻防实验室）	4	4
任子行网络技术股份有限公司	3	3
福建省海峡信息技术公司	2	2
北京明朝万达科技股份有限公司（安元实验室）	1	1
CNCERT 吉林分中心	4	4
CNCERT 新疆分中心	2	2
CNCERT 浙江分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 海南分中心	1	1
个人	56	56
报送总计	2621	456

本周漏洞按类型和厂商统计

本周，CNVD 收录了 257 个漏洞。其中应用程序漏洞 180 个，网络设备漏洞 28 个，WEB 应用漏洞 25 个，操作系统漏洞 21 个，安全产品漏洞 3 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	180
网络设备漏洞	28
WEB 应用漏洞	25
操作系统漏洞	21
安全产品漏洞	3

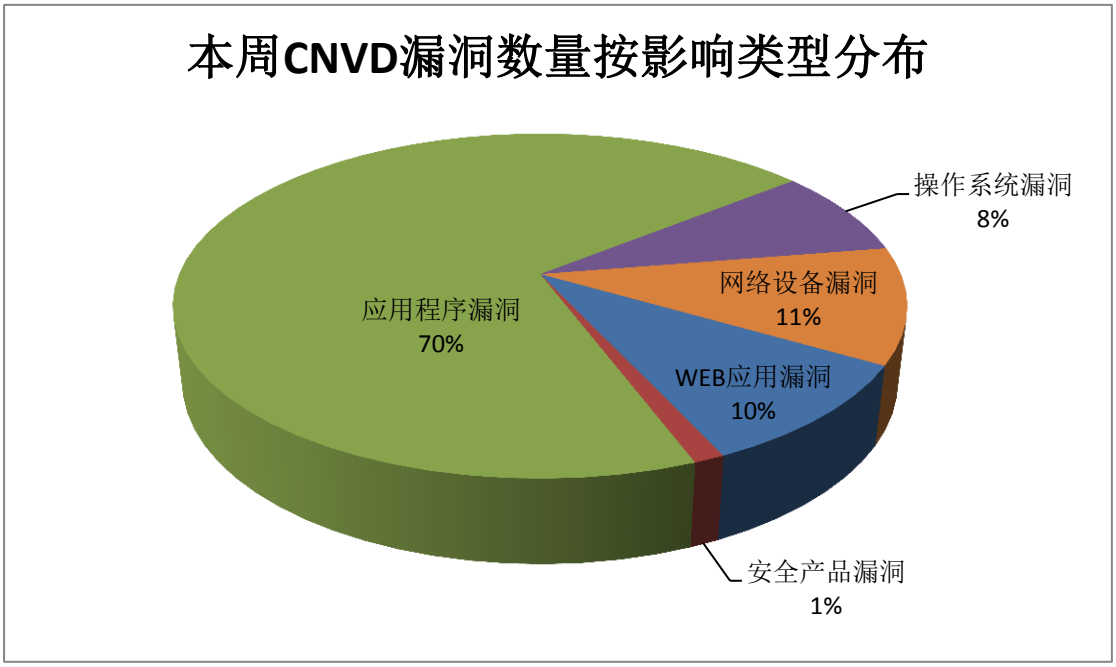

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、Microsoft 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	Adobe	26	10%
2	Google	17	6%
3	Microsoft	15	6%
4	Huawei	11	4%
5	IBM	9	4%
6	CloudBees	6	2%
7	ONELAN	5	2%
8	D-Link	4	2%
9	ADB	3	1%
10	其他	161	63%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，20 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“多款 OSIsoft PI 产品远程代码执行漏洞、Android Qualcom power_stats debugfs node 权限提升漏洞、ADB Broadband Gateways/Routers 权限提升漏洞、

Google Android Media framework 权限提升漏洞（CNVD-2018-13166）、ADB Broadband Gateways/Routers 本地 root 越狱漏洞”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/

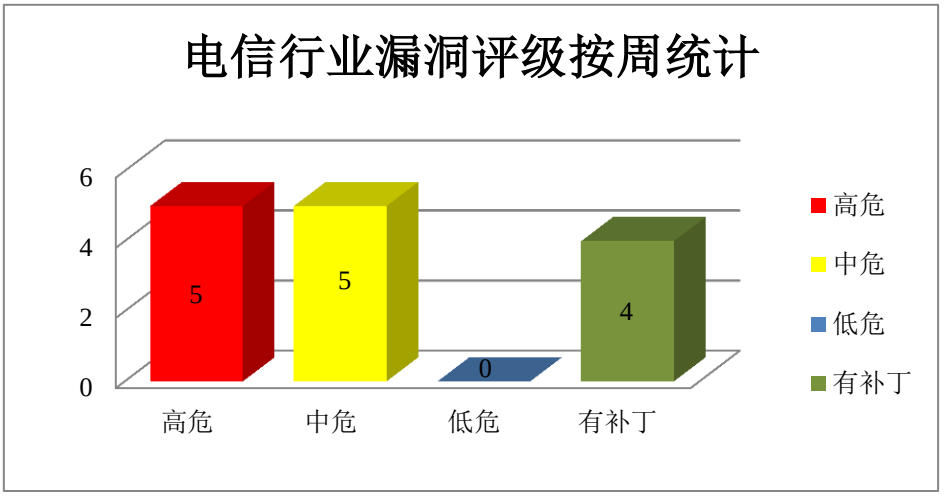

图 3 电信行业漏洞统计

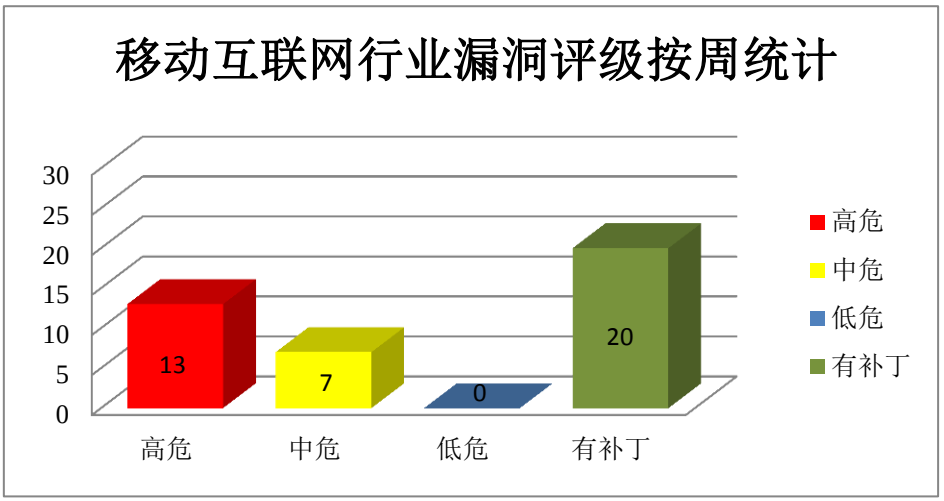

图 4 移动互联网行业漏洞统计

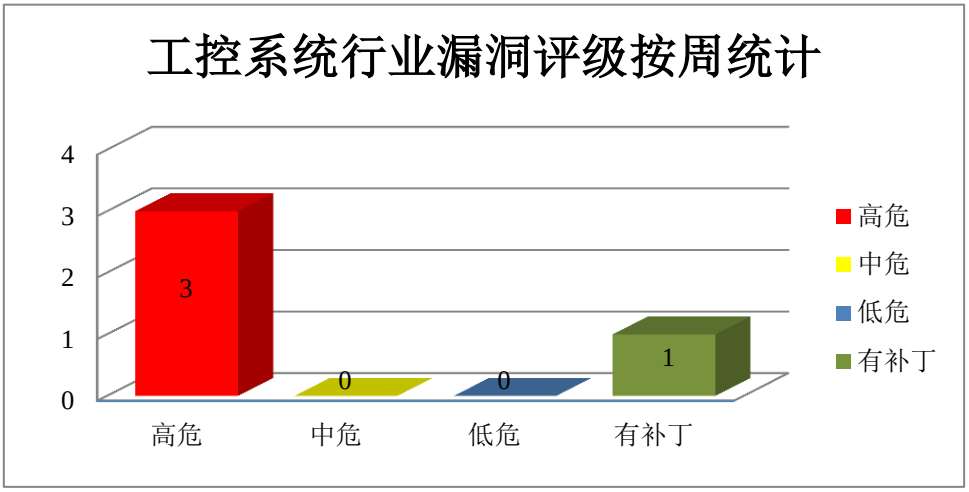

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在堆溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 堆溢出漏洞（CNVD-2018-12938、CNVD-2018-12942、CNVD-2018-12943、CNVD-2018-13063、CNVD-2018-13064、CNVD-2018-13065、CNVD-2018-13066、CNVD-2018-13067）。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-2018-12938

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12942

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12943

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13063

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13064

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13065

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13066

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13067

2、Google 产品安全漏洞

Android 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。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android MediaTek 组件权限提升漏洞（CNVD-2018-13158、CNVD-2018-13159、CNVD-2018-13160、CNVD-2018-13163、CNVD-2018-13164、CNVD-2018-13165、CNVD-2018-13167、CNVD-2018-13168）。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-2018-13158

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13159

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13160

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13163

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13164

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13165

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13167

http://www.cnvd.org.cn/flaw/show/CNVD-2018-13168

3、Microsoft 产品安全漏洞

Microsoft Windows 10 是美国微软（Microsoft）公司发布的一套新一代跨平台操作系统，它适用于 PC 和笔记本电脑、平板电脑以及手机等设备。Edge 是其中的一个系统附带的默认浏览器。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，从而可获得与当前用户相同的用户权限。

CNVD 收录的相关漏洞包括：Microsoft Edge 内存破坏漏洞（CNVD-2018-12883、CNVD-2018-12884、CNVD-2018-12885、CNVD-2018-12886、CNVD-2018-12887、CNVD-2018-12888）、Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2018-12889、CNVD-2018-12890）。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-2018-12883

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12884

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12885

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12886

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12887

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12888

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12889

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12890

4、Huawei 产品安全漏洞

Huawei Mate 8、Huawei Mate 9、Huawei Mate 10、Huawei LYO-L21、Huawei Berlin-L21HN 和 Prague-AL00A 等都是智能手机产品。Huawei IPS Module 是一款 IPS 安全设备。NGFW Module 是一款防火墙设备。NIP6300 等是下一代入侵防御系统。本

周，该产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行远程代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Huawei Mate 10 拒绝服务漏洞、多款 Huawei 产品内存泄露漏洞（CNVD-2018-12787）、多款 Huawei 手机信息泄露漏洞、Huawei Mate 9 Pro GPU 驱动任意内存释放漏洞、多款 Huawei 手机拒绝服务漏洞、Huawei Mate 9 Pro 手机短信息模块拒绝服务漏洞、Huawei LYO-L21 手机权限提升漏洞、Huawei Mate 10 手机内存错误引用漏洞。其中，“多款 Huawei 手机信息泄露漏洞、Huawei Mate 9 Pro GPU 驱动任意内存释放漏洞、Huawei Mate 9 Pro 手机短信息模块拒绝服务漏洞、Huawei LYO-L21 手机权限提升漏洞”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-2018-12788
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12787
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12842
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12844
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12843
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12846
http://www.cnvd.org.cn/flaw/show/CNVD-2018-12845
http://www.cnvd.org.cn/flaw/show/CNVD-2018-13042

5、D-Link DIR-620 路由器操作系统命令注入漏洞

D-link DIR-620 是友讯（D-Link）公司的一款无线路由器产品。本周，D-link DIR-620 被披露存在命令注入漏洞，该漏洞源于程序未能正确的处理传递到 index.cgi 文件的’res_buf’参数。攻击者可利用该漏洞执行操作系统命令。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-2018-12850

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-2018-12782	ADB Broadband Gateways/Routers 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.adbglobal.com/
CNVD-2018-12822	多款 Qualcomm 产品 ADSP RPC 组件内存错误引用漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.qualcomm.com/company/product-security/bulletins

CNVD-2018-12841	VLC media player 任意代码执行漏洞（CNVD-2018-12841）	高	用户可联系供应商获得补丁信息：https://get.videolan.org/vlc/3.0.3/win64/vlc-3.0.3-win64.exe
CNVD-2018-12875	Marlin 缓冲区错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/MarlinFirmware/Marlin/pull/10925
CNVD-2018-12925	Drupal Clientside Validation 模块远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.drupal.org/node/2907118
CNVD-2018-13072	ONELAN CMS 任意文件上传漏洞	高	用户可联系供应商获得补丁信息：https://onelan.com/products/publisher-cms/
CNVD-2018-13101	ELO ELOenterprise 和 ELOprofessional Access Manager 组件 SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.elo.com/
CNVD-2018-12932	多款 OSIsoft PI 产品远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ics-cert.us-cert.gov/advisories/ICSA-17-192-05
CNVD-2018-12823	多款 Qualcomm 产品权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.qualcomm.com/company/product-security/bulletins
CNVD-2018-13171	SaltStack Salt 欺骗漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.saltstack.com/en/2017.7/topics/releases/2016.3.6.html

小结：本周，Adobe 被披露存在堆溢出漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Microsoft、Huawei 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行远程代码或发起拒绝服务攻击等。另外，D-Link DIR-620 路由器操作系统命令注入漏洞，攻击者可利用该漏洞执行操作系统命令。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. 微软对外披露两个 0day 漏洞

近日，微软对外披露了两个 0day 漏洞详情，其中一个漏洞存在 Adobe 阅读器中，可被利用导致任意代码执行；另一个漏洞则允许任意代码在 Windows kernel 内存中提权执行。微软称由于该漏洞利用目前还处于初期阶段，且官方都已发布了补丁，建议大家及时进行安装。同时，建议排查初期样本的 IOC（文末附修复补丁链接和 IOC）。

参考链接：http://www.freebuf.com/vuls/176703.html

2. 幽灵安全漏洞 Spectre 1.1 新变种曝光

近日，两位安全研究人员发布了一篇揭露 “幽灵”（Spectre）安全漏洞新变种的论文，因其会产生投机性的缓冲区溢出。对于处理器厂商来说，年初被曝光的该漏洞、以及后续陆续出现的多个其它变种。而最新的 Spectre 1.1 漏洞，则利用了投机性的缓冲区溢出。

参考链接：https://news.softpedia.com/news/new-variant-of-spectre-security-flaw-discovered-speculative-buffer-overflows-521915.shtml

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