国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 5 月 7 日-2018 年 5 月 13 日 **2018 年第 19 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 260 个，其中高危漏洞 62 个、中危漏洞 184 个、低危漏洞 14 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 59 个（占 23%），其中互联网上出现“D-Link DIR-601 存在信息泄露漏洞、WordPress wunderfarm WF Cookie Consent 插件跨站脚本漏洞”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 614 个，与上周（534 个）环比增长 15%。

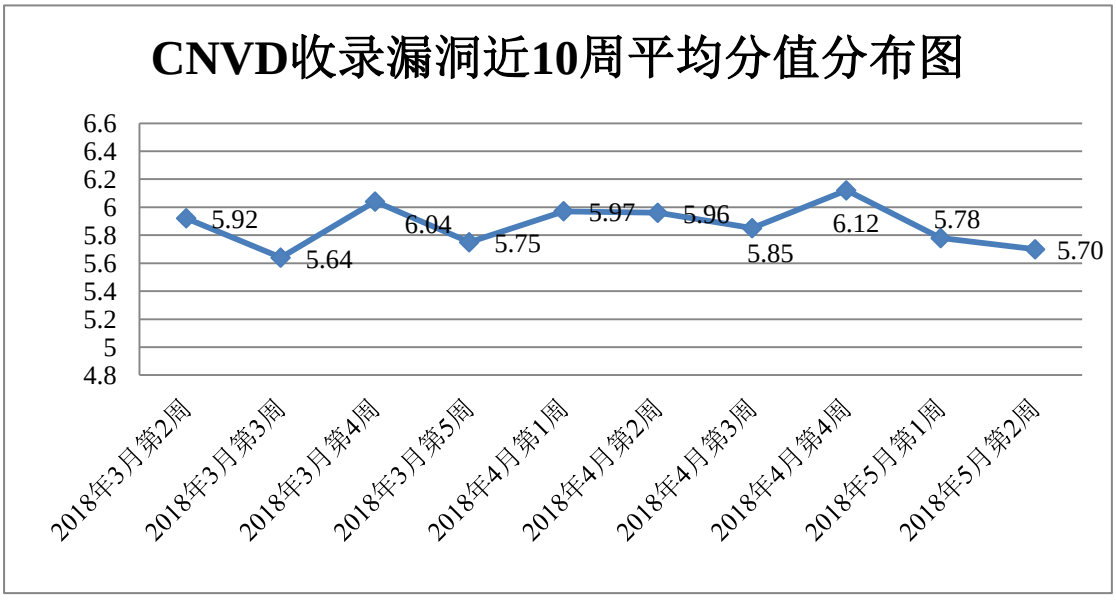

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、北京天融信网络安全技术有限公司、哈尔滨安天科技股份有限公司、中国电信集团系统集成有限责任公司、

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）、南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、广西网信信息安全等级保护测评有限公司、安徽锋刃信息科技有限公司、山石网科通信技术有限公司、福建省海峡信息技术有限公司、北京同余科技有限公司及其他个人白帽子向 CNVD 提交了 614 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 453 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
蓝盾信息安全技术有限公司	1708	1
北京天融信网络安全技术有限公司	295	1
漏洞盒子	239	239
360 网神（补天平台）	214	214
哈尔滨安天科技股份有限公司	205	0
中国电信集团系统集成有限责任公司	144	0
新华三技术有限公司	130	0
华为技术有限公司	129	0
北京数字观星科技有限公司	52	0
恒安嘉新(北京)科技股份公司	50	0
北京神州绿盟科技有限公司	32	0
北京无声信息技术有限公司	25	0
杭州安恒信息技术有限公司	8	0
北京知道创宇信息技术有限公司	2	1
西安四叶草信息技术有限公司	2	2
四川虹微技术有限公司（子午攻防实验室）	14	14
南京联成科技发展股份有限公司	7	7

中新网络信息安全股份有限公司	7	7
广西网信信息安全等级保护测评有限公司	3	3
安徽锋刃信息科技有限公司	2	2
山石网科通信技术有限公司	1	1
福建省海峡信息技术有限公司	1	1
北京同余科技有限公司	1	1
CNCERT 吉林分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 新疆分中心	1	1
个人	116	116
报送总计	3391	614

本周漏洞按类型和厂商统计

本周，CNVD 收录了 260 个漏洞。其中应用程序漏洞 188 个，网络设备漏洞 26 个，WEB 应用漏洞 22 个，操作系统漏洞 17 个，安全产品漏洞 4 个，数据库漏洞 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	188
网络设备漏洞	26
WEB 应用漏洞	22
操作系统漏洞	17
安全产品漏洞	4
数据库漏洞	3

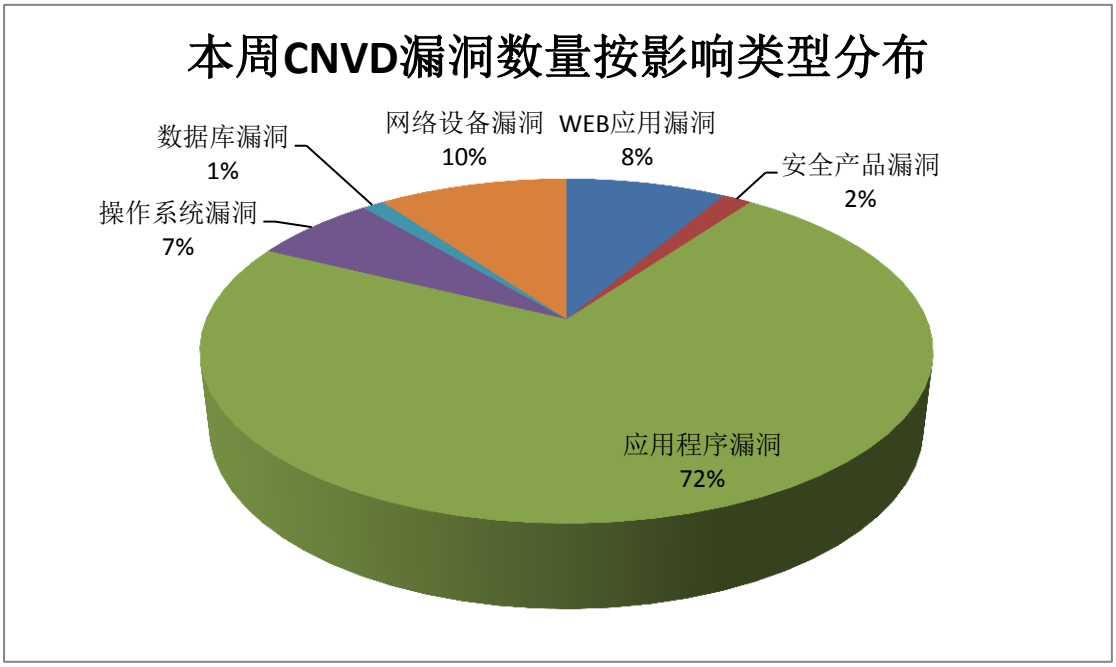

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、IBM、Google 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	Oracle	72	28%
2	IBM	18	7%
3	Google	16	6%
4	Cisco	13	5%
5	Adobe	10	4%
6	D-Link	7	3%
7	Flexense	6	2%
8	Cms made simple	5	2%
9	Red Hat	5	2%
10	其他	108	41%

本周行业漏洞收录情况

本周，CNVD 收录了 19 个电信行业漏洞，12 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“ymantec Norton Core router 命令注入漏洞、GPon 路由器远程命令执行漏洞、多款 Sierra Wireless 产品任意代码执行漏洞、Adobe Digital Edi

tions 缓冲区溢出漏洞（CNVD-2018-09333）、Philips Brilliance CT Scanners 硬编码证书漏洞”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/

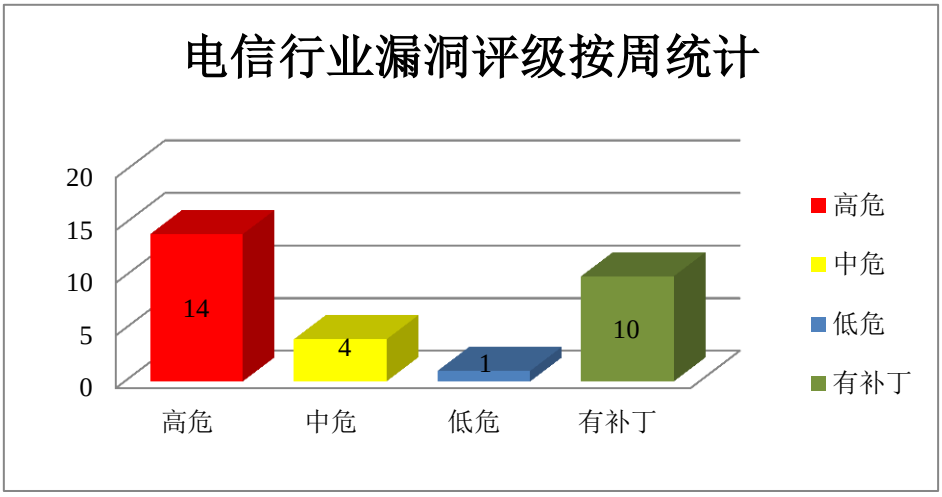

图 3 电信行业漏洞统计

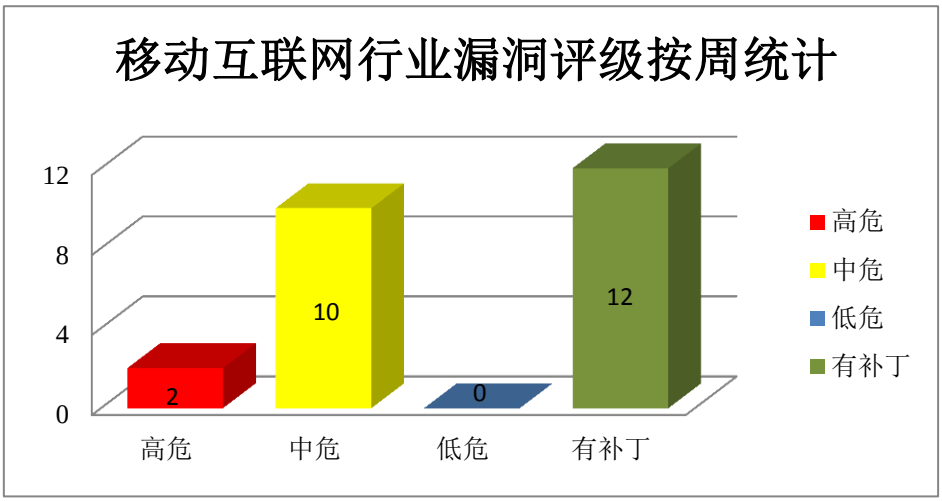

图 4 移动互联网行业漏洞统计

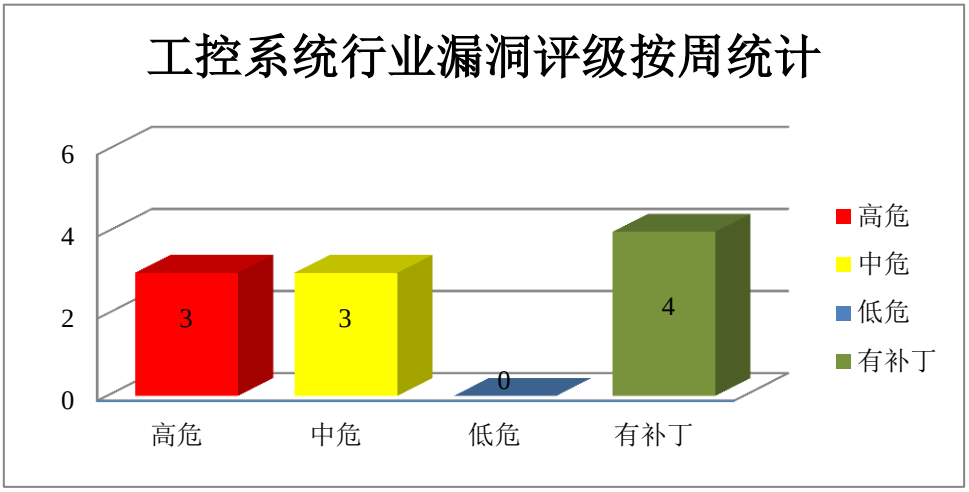

图 5 工控行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。Flash 是其中的一个用于处理 Flash 的插件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome Flash 内存错误引用漏洞、Google Chrome Flash 内存错误引用漏洞（CNVD-2018-09117）、Google Chrome 权限提升漏洞（CNVD-2018-09120、CNVD-2018-09121）、Google Chrome V8 竞争条件漏洞、Google Chrome V8 类型混淆漏洞（CNVD-2018-09122）、Google Chrome V8 整数溢出漏洞、Google Chrome 设计漏洞。除“Google Chrome V8 整数溢出漏洞、Google Chrome 设计漏洞”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-2018-09118

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09117

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09120

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09121

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09119

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09122

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09123

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09125

2、Adobe 产品安全漏洞

Adobe Digital Editions（DE）是美国奥多比（Adobe）公司的一套电子书阅读管理

软件。Adobe Flash Player 是多媒体程序播放器。Adobe Creative Cloud 是包括平面设计、影片编辑、网页开发应用的云端套装软件。Adobe InDesign CC 是一套排版编辑应用程序。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提升权限等。

CNVD 收录的相关漏洞包括：Adobe Creative Cloud 权限提升漏洞、Adobe Creative Cloud 权限提升漏洞（CNVD-2018-09211）、Adobe Digital Editions 缓冲区溢出漏洞（CNVD-2018-09333、CNVD-2018-09334）、Adobe Flash Player 代码执行漏洞（CNVD-2018-09032）、Adobe Flash Player 类型混淆远程代码执行漏洞（CNVD-2018-09212）、Adobe InDesign CC 内存破坏漏洞、Adobe PhoneGap Push 插件代码执行漏洞。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-2018-09213
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09211
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09333
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09334
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09032
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09212
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09336
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09335

3、Oracle 产品安全漏洞

Oracle Sun Solaris 是最初由 Sun Microsystems 开发的 Unix 操作系统。Oracle Hospitality Simphony 提供现代化的用户体验。本周，上述产品被披露存在安全漏洞，攻击者可利用该漏洞影响机密性、完整性及可用性。

CNVD 收录的相关漏洞包括：Oracle Hospitality Simphony 存在未明漏洞（CNVD-2018-09086、CNVD-2018-09082、CNVD-2018-09083、CNVD-2018-09084）、Oracle Sun Solaris 存在未明漏洞（CNVD-2018-09050、CNVD-2018-09045、CNVD-2018-09047、CNVD-2018-09048）。其中，“Oracle Hospitality Simphony 存在未明漏洞（CNVD-2018-09084）、Oracle Sun Solaris 存在未明漏洞（CNVD-2018-09050、CNVD-2018-09045）”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-2018-09086
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09082
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09083
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09084
http://www.cnvd.org.cn/flaw/show/CNVD-2018-09050

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09045

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09047

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09048

4、D-Link 产品安全漏洞

D-Link DSL-3782、DIR-601 等都是友讯（D-Link）公司的无线路由器产品。本周，上述产品被披露存在信息泄露、代码执行和缓冲区溢出漏洞，攻击者可利用漏洞泄露敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：D-Link DIR-601 存在信息泄露漏洞、D-Link DIR-615 远程代码执行漏洞、D-Link DSL-3782 代码执行漏洞、D-Link DSL-3782 缓冲区溢出漏洞（CNVD-2018-09178、CNVD-2018-09179、CNVD-2018-09180、CNVD-2018-09181、CNVD-2018-09182）。除“D-Link DIR-601 存在信息泄露漏洞”外，其余漏洞的综合评级为“高危”。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-2018-09185

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08994

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09195

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09178

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09179

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09180

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09181

http://www.cnvd.org.cn/flaw/show/CNVD-2018-09182

5、Apache Derby 外部控制输入漏洞

Apache Derby 是美国阿帕奇（Apache）软件基金会开发的一套开源的数据库管理系统。本周，Apache 被披露存在外部控制输入漏洞，远程攻击者可通过发送特制的网络数据包利用该漏洞启动用户控制的数据库（位置和内容）。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-2018-09148

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-2018-09057	TunnelBear for Windows 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.tunnelbear.com/
CNVD-2018-09147	Pivotal Spring Cloud SSO Connector 身份验证漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			https://pivotal.io/security/cve-2018-1256
CNVD-2018-09151	多款 Sierra Wireless 产品任意代码执行漏洞（CNVD-2018-09151）	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.sierrawireless.com/
CNVD-2018-09153	多款 Sierra Wireless 产品任意代码执行漏洞	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.sierrawireless.com/
CNVD-2018-09165	GPon 路由器远程命令执行漏洞	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：http://www.dasannetworks.com
CNVD-2018-09190	多款 Lenovo 产品代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.lenovo.com/us/zh/solutions/len-20241
CNVD-2018-09230	GPON Home Routers 安全绕过漏洞	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：http://www.dasannetworks.com
CNVD-2018-09303	RSA 认证管理器存在拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://pilot.search.dell.com
CNVD-2018-09325	KDE Kwallet kwallet-pam 本地权限获取漏洞	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.dellemc.com/
CNVD-2018-09324	Dell EMC Unity Operating Environment 操作系统命令注入漏洞	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.dellemc.com/

小结：本周， Google 被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或造成拒绝服务等。此外，Adobe、Oracle、D-Link 等多款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、提升权限或进行跨站脚本攻击等。另外，Apache 被披露存在外部控制输入漏洞，远程攻击者可通过发送特制的网络数据包利用该漏洞启动用户控制的数据库（位置和内容）。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. OpenFlow 交换机协议曝身份验证漏洞

5 月 11 日讯 作为一项早期软件定义网络协议，OpenFlow 中曝出一项安全漏洞，这项漏洞年代久远、无处不在，且很难在短时间内得到修复。研究人员们表示，在未对协议本身（以及众多第三方软件）进行更新的情况下，OpenFlow 连接可以通过为交换机提供惟一 TLS 证书的方式将交换机 DPID 与控制器列入白名单，并允许控制器验证

DPID 及其证书。

参考链接：https://www.easyaq.com/news/573388844.shtml

2. Windows、macOS 和 Linux 系统正遭受重大安全漏洞影响

Windows、macOS、Linux、FreeBSD、VMware 和 Xen 等系统目前正受到一处重大安全漏洞的影响，而该漏洞是由于操作系统开发者曲解了英特尔和 AMD 两大芯片厂商的调试文档所致。该漏洞源自操作系统和管理程序处理 CPU 特定调试功能的方式。对于 Linux 操作系统而言，该漏洞可能导致系统崩溃，也允许黑客提高“访客”账户的访问权限。

参考链接：https://www.easyaq.com/news/721010656.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