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 28 日-2018 年 6 月 03 日　　2018 年第 22 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 127 个、中危漏洞 165 个、低危漏洞 17 个。漏洞平均分值为 6.31。本周收录的漏洞中，涉及 0day 漏洞 81 个（占 26%），其中互联网上出现“D-Link DSL-3782 Login Panel 未授权操作漏洞、Samsung S7 Edge 整数溢出漏洞”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 465 个，与上周（458 个）环比增长 2%。

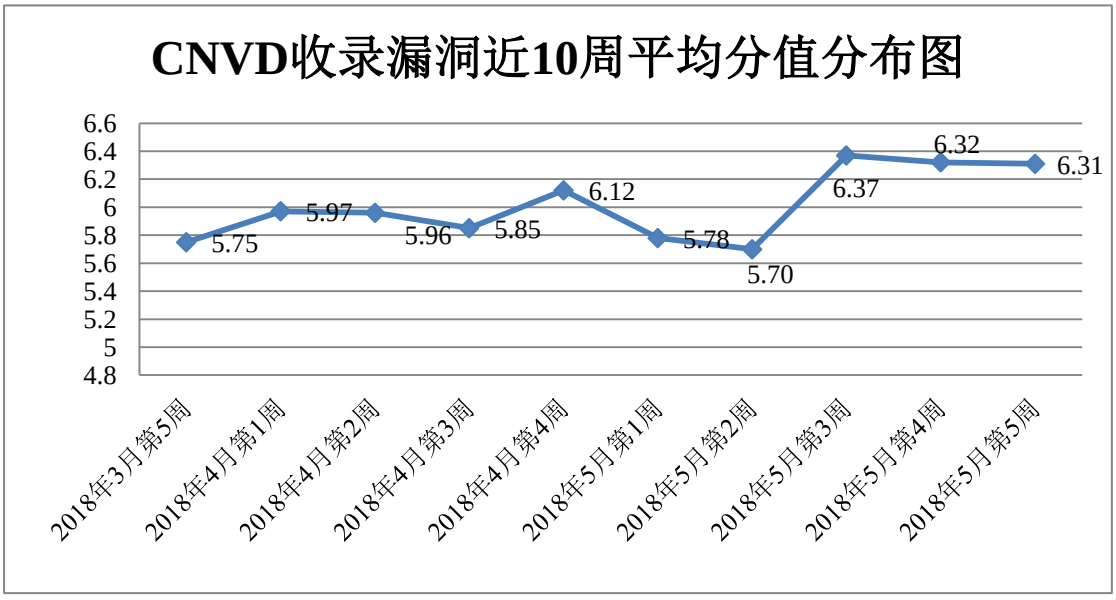

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、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、北京天融信网络安全技术有限公司、华为

技术有限公司等单位报送公开收集的漏洞数量较多。南京联成科技发展股份有限公司、四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、上海观安信息技术股份有限公司、广州万方计算机科技有限公司、济南三泽信息安全测评有限公司、北京明朝万达科技股份有限公司（安元实验室）、山东省网络与信息安全测评中心及其他个人白帽子向 CNVD 提交了 465 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 183 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	688	0
沈阳东软系统集成工程有限公司	428	0
哈尔滨安天科技股份有限公司	214	0
360 网神（补天平台）	196	196
北京天融信网络安全技术有限公司	187	3
华为技术有限公司	150	0
新华三技术有限公司	98	0
北京神州绿盟科技有限公司	68	0
恒安嘉新(北京)科技股份公司	62	0
北京数字观星科技有限公司	55	0
中国电信集团系统集成有限责任公司	55	0
漏洞盒子	47	47
北京启明星辰信息安全技术有限公司	40	0
杭州安恒信息技术有限公司	23	0
厦门服云信息科技有限公司	22	0
北京无声信息技术有限公司	7	0
北京知道创宇信息技术有限公司	1	1

南京联成科技发展股份有限公司	28	28
四川虹微技术有限公司（子午攻防实验室）	14	14
中新网络信息安全股份有限公司	7	7
上海观安信息技术股份有限公司	3	3
广州万方计算机科技有限公司	3	3
济南三泽信息安全测评有限公司	3	3
北京明朝万达科技股份有限公司（安元实验室）	2	2
山东省网络与信息安全测评中心	1	1
CNCERT 上海分中心	11	11
CNCERT 山西分中心	9	9
CNCERT 甘肃分中心	7	7
CNCERT 河北分中心	6	6
CNCERT 湖南分中心	6	6
CNCERT 宁夏分中心	5	5
CNCERT 广东分中心	5	5
CNCERT 天津分中心	5	5
CNCERT 吉林分中心	2	2
CNCERT 贵州分中心	1	1
个人	100	100
报送总计	2559	465

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 194 个，WEB 应用漏洞 53 个，操作系统漏洞 31 个，网络设备漏洞 18 个，数据库漏洞 10 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	194
WEB 应用漏洞	53
操作系统漏洞	31
网络设备漏洞	18
数据库漏洞	10
安全产品漏洞	3

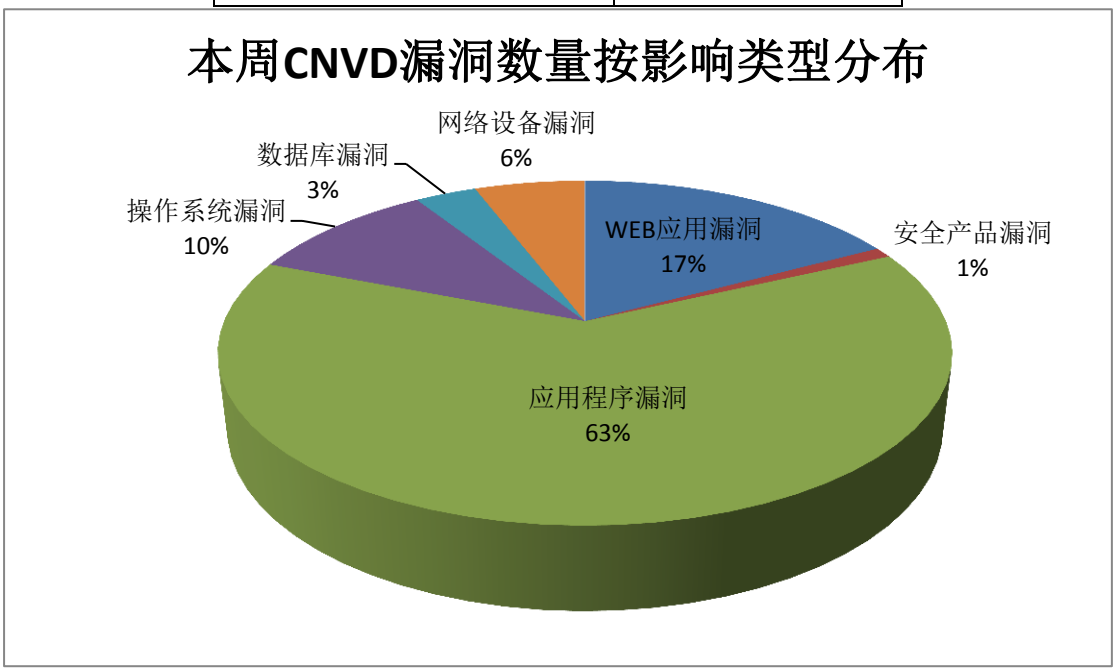

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、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	Microsoft	29	9%
2	IBM	23	7%
3	Google	22	7%
4	Adobe	16	5%
5	Foxit	12	4%
6	WordPress	8	3%
7	Cisco	6	2%
8	Oracle	6	2%
9	Trend Micro	6	2%

10	其他	181	59%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，28 个移动互联网行业漏洞，16 个工控行业漏洞（如下图所示）。其中，“DCCE MAC1100 PLC 存在远程代码上传漏洞、Advantech WebAccess 栈缓冲区溢出漏洞（CNVD-2018-10713）、Google Android System 权限提升漏洞（CNVD-2018-10692）、eVestigator Forensic PenTester 远程代码执行漏洞、IBM DB2 for Linux、UNIX 和 Windows 缓冲区溢出漏洞”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/

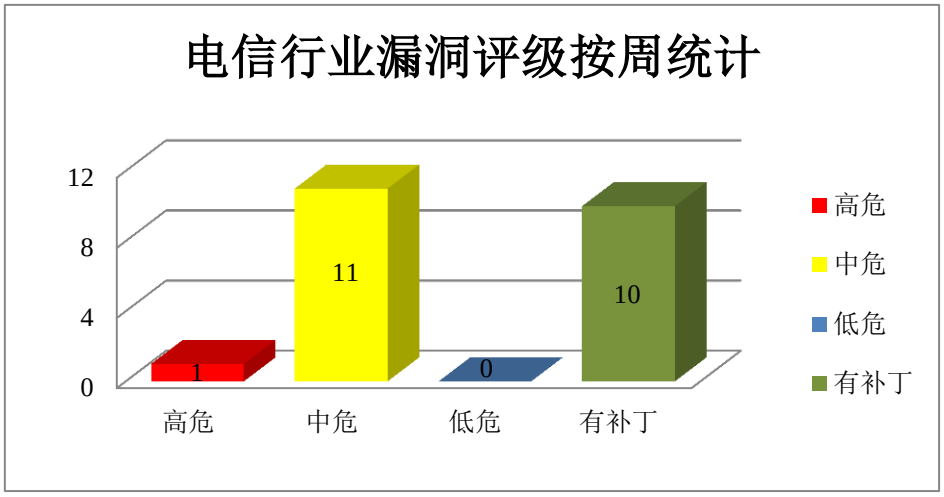

图 3 电信行业漏洞统计

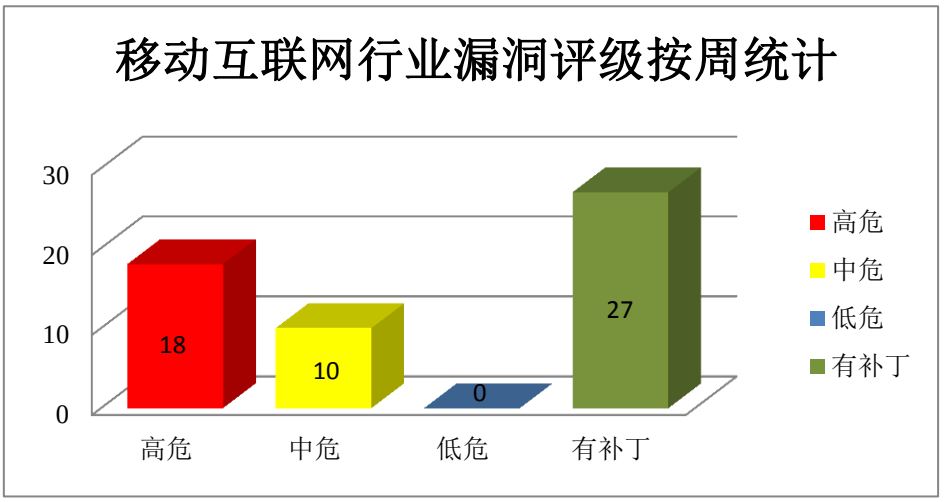

图 4 移动互联网行业漏洞统计

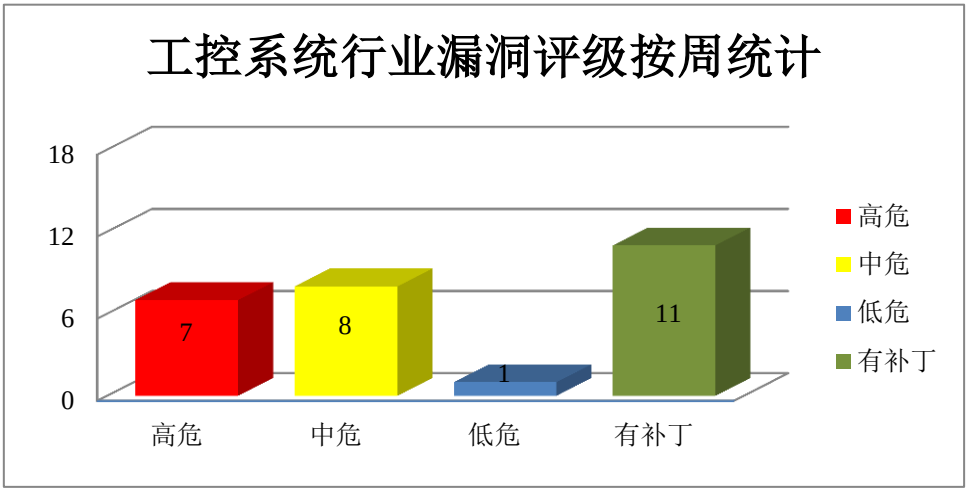

图 5 工控行业漏洞统计

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

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 Qualcomm 组件权限提升漏洞（CNVD-2018-10681、CNVD-2018-10682、CNVD-2018-10683、CNVD-2018-10684、CNVD-2018-10685、CNVD-2018-10686、CNVD-2018-10687、CNVD-2018-10688），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-2018-10681

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10682

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10683

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10684

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10685

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10686

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10687

http://www.cnvd.org.cn/flaw/show/CNVD-2018-10688

2、Microsoft 产品安全漏洞

M Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。Microsoft Office 2010 SP2 是一款办公软件套件产品。Excel 2010 SP2 是 Office 套件中的一套电子表格处理软件。Microsoft Edge 是一款流行的 WEB 浏览器。本周，上

述产品被披露存在远程代码执行、内存破坏和权限提升漏洞，攻击者可利用漏洞执行任意代码、提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Office 远程代码执行漏洞（CNVD-2018-10431、CNVD-2018-10439、CNVD-2018-10440）、Microsoft Excel 远程代码执行漏洞（CNVD-2018-10432、CNVD-2018-10433）、Microsoft Edge 脚本引擎远程内存破坏漏洞（CNVD-2018-10735、CNVD-2018-10736）、Microsoft Exchange Server 权限提升漏洞。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-2018-10431
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10439
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10440
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10432
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10433
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10735
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10736
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10434

3、Adobe 产品安全漏洞

Adobe Reader 是美国 Adobe 公司开发的一款 PDF 文件阅读软件。Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。本周，上述产品被披露存在内存错误引用漏洞，攻击者可利用该漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存错误引用漏洞（CNVD-2018-10460、CNVD-2018-10461、CNVD-2018-10462、CNVD-2018-10463、CNVD-2018-10464、CNVD-2018-10465、CNVD-2018-10466、CNVD-2018-10467）。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-2018-10460
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10461
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10462
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10463
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10464
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10465
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10466
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10467

4、IBM 产品安全漏洞

IBM FlashSystem 产品是将数据存储在闪存上的企业计算机数据存储系统。 IBM

DB2 是美国 IBM 公司的一套关系型数据库管理系统。IBM UrbanCode Deploy（UCD）是美国 IBM 公司的一套应用自动化部署工具。本周，该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或执行任意代码等。

CNVD 收录的相关漏洞包括：IBM DB2 for Linux、UNIX 和 Windows 缓冲区溢出漏洞、IBM DB2 缓冲区溢出漏洞（CNVD-2018-10801、CNVD-2018-10804、CNVD-2018-10805）、IBM FlashSystem 任意文件覆盖漏洞、IBM Security QRadar SIEM SQL 注入漏洞（CNVD-2018-10458）、IBM Security QRadar SIEM 目录遍历漏洞（CNVD-2018-10457）、IBM UrbanCode Deploy 信息泄露漏洞（CNVD-2018-10455），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-2018-10563
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10801
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10804
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10805
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10704
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10458
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10457
http://www.cnvd.org.cn/flaw/show/CNVD-2018-10455

5、Apache Hadoop 权限提升漏洞（CNVD-2018-10426）

Apache Hadoop 是美国阿帕奇（Apache）软件基金会的一套开源的分布式系统基础架构。本周，Apache 被披露存在权限提升漏洞，攻击者可利用漏洞升级为 yarn 用户的用户，并以 root 用户身份运行任意命令。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-2018-10426

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-2018-10427	Quassel 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://quassel-irc.org/taxonomy/term/7
CNVD-2018-10651	Moodle 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://moodle.org/mod/forum/discuss.php?d=371199
CNVD-201	Octopus Deploy 安全限制绕过	高	目前厂商已发布升级补丁以修复漏

8-10663	漏洞		洞，补丁获取链接：https://github.com/OctopusDeploy/Issues/issues/4454
CNVD-2018-10671	selenium-download 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://github.com/groupon/selenium-download/releases
CNVD-2018-10673	sequelize SQL 注入漏洞	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/sequelize/sequelize/issues/5671
CNVD-2018-10672	aerospike 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.npmjs.com/package/aerospike
CNVD-2018-10674	waterline-sequel SQL 注入漏洞	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/balderdashy/waterline-sequel/pull/66
CNVD-2018-10699	Fortinet FortiWLC 硬编码账户漏洞（CNVD-2018-10699）	高	厂商已发布漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-17-274
CNVD-2018-10700	Fortinet FortiWLC 硬编码账户漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-17-274
CNVD-2018-10794	Git 任意代码执行漏洞（CNVD-2018-10794）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git-scm.com/

小结：本周， Google 被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，Microsoft、Adobe、IBM 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，Apache 被披露存在权限提升漏洞，攻击者可利用漏洞升级为 yarn 用户的用户，并以 root 用户身份运行任意命令。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. 美国必康美德医疗设备曝多个安全漏洞

最近，美国 ICS-CERT 发布并修改了一份名为《美国必康美德 TotalAlert Scroll 医用空气系统》（ICSMA-18-144-01）的公告，警告称在美国必康美德公司 TotalAlert S

croll 医用空气系统的医疗设备中发现了三个安全漏洞。攻击者可利用 TotalAlert Scroll 医用空气系统 web 应用程序中的漏洞，查看和修改一些设备信息和 web 应用程序设置。这些漏洞由安全研究员马克西姆·鲁普向美国国土安全部（DHS）的国家网络安全和通信整合中心（NCCIC）报告，由 NCCIC 下的 ICS-CERT 负责发出警报公告。

参考链接：https://www.easyaq.com/news/449826044.shtml

2. Windows 曝 0day 远程代码执行漏洞

近日，windows 系统又发现一起 0day 漏洞，该漏洞是由系统中的 JScript 组件造成的，允许远程攻击者在用户的 PC 上执行恶意代码，虽然微软并未提供计划推出补丁的确切时间表，但一位发言人表明他们正在进行修复。此漏洞允许远程攻击者在 Microsoft Windows 的易受攻击的安装上执行任意代码。目前，ZDI 专家建议用户不要允许依赖 JScript 组件的应用程序（如 Internet Explorer，wscript.exe 等）处理不受信任的 JS 代码或文件。

参考链接：https://www.easyaq.com/news/1234486782.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