

信息安全漏洞周报

2018 年 7 月 2 日-2018 年 7 月 8 日

2018 年第 27 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 179 个，其中高危漏洞 55 个、中危漏洞 108 个、低危漏洞 16 个。漏洞平均分为 5.82。本周收录的漏洞中，涉及 0day 漏洞 34 个（占 19%），其中互联网上出现“WordPress Product Enquiry for WooCommerce 插件跨站脚本漏洞、Microsoft Windows EMET XML 外部实体注入漏洞”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 283 个，与上周（393 个）环比下降 28%。

CNVD收录漏洞近10周平均分分布图

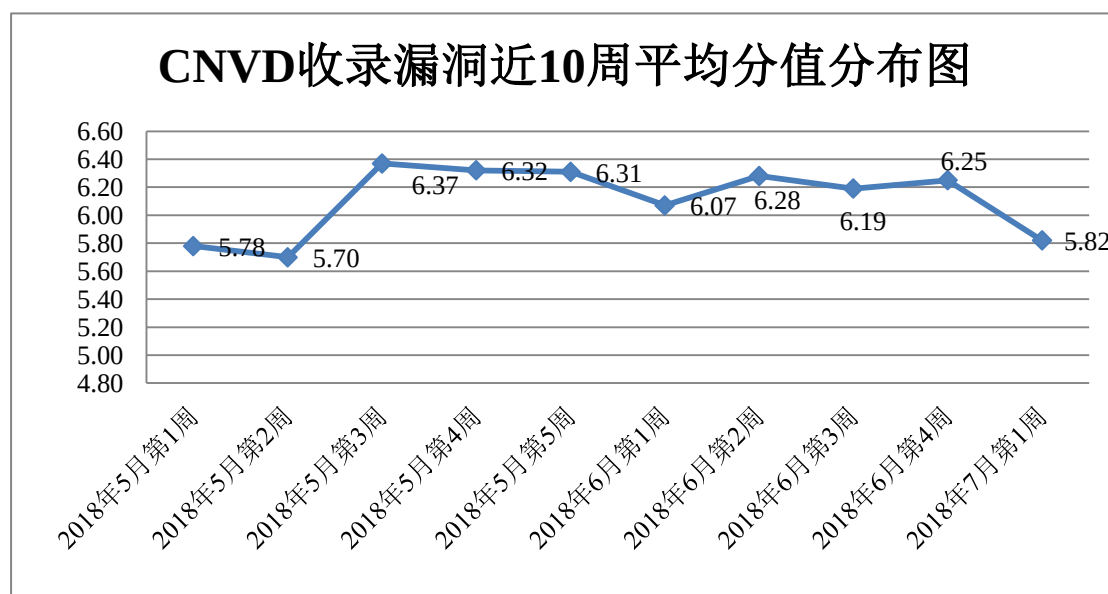


图 1 CNVD 收录漏洞近 10 周平均分分布图

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、杭州安恒信息技术有限公司、哈尔滨安天科技股份有限公司、华为技术有限公司、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。上海银基信息安全技术股份有限公司、中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、福建六壬网安股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、山石网科通信技术有限公司、安徽锋刃信息科技有限公司、北京国舜科技股份有限公司、南京联成科技发展有限公司、上海纽盾科技股份有限公司、济南三泽信息安全测评有限公司及其他个人白帽子向 CNVD 提交了 283 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 133 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	379	1
杭州安恒信息技术有限公司	306	0
哈尔滨安天科技股份有限公司	249	0
华为技术有限公司	160	0
阿里云计算有限公司	119	0
新华三技术有限公司	119	0
360 网神（补天平台）	115	115
北京神州绿盟科技有限公司	98	0
北京数字观星科技有限公司	68	0
恒安嘉新(北京)科技股份有限公司	51	0
中国电信集团系统集成有限责任公司	41	0
深圳市深信服电子科技有限公司	38	0
漏洞盒子	18	18
厦门服云信息科技有限公司	9	0
北京无声信息技术有限公司	6	0
北京知道创宇信息技术有限公司	5	2

上海银基信息安全技术股份有限公司	16	16
中新网络信息安全股份有限公司	10	10
四川虹微技术有限公司 (子午攻防实验室)	7	7
福建六壬网安股份有限公司	3	3
北京明朝万达科技股份有限公司 (安元实验室)	2	2
山石网科通信技术有限公司	1	1
安徽锋刃信息科技有限公司	1	1
北京国舜科技股份有限公司	1	1
南京联成科技发展股份有限公司	1	1
上海纽盾科技股份有限公司	1	1
济南三泽信息安全测评有限公司	1	1
CNCERT 吉林分中心	5	5
CNCERT 河北分中心	5	5
CNCERT 新疆分中心	4	4
CNCERT 贵州分中心	3	3
CNCERT 广东分中心	3	3
CNCERT 海南分中心	2	2
CNCERT 陕西分中心	1	1
个人	80	80
报送总计	1928	283

本周漏洞按类型和厂商统计

本周，CNVD 收录了 179 个漏洞。其中应用程序漏洞 88 个，操作系统漏洞 48 个，WEB 应用漏洞 23 个，网络设备漏洞 17 个，数据库漏洞 2 个，安全产品漏洞 1 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	88
操作系统漏洞	48
WEB 应用漏洞	23
网络设备漏洞	17
数据库漏洞	2
安全产品漏洞	1

本周CNVD漏洞数量按影响类型分布

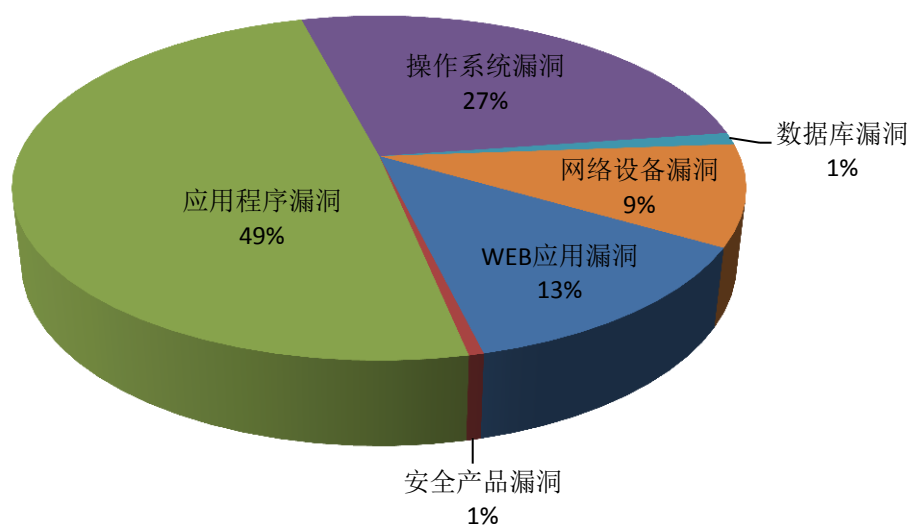


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、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	Google	31	17%
2	IBM	27	15%
3	Microsoft	20	11%
4	Apache	11	6%
5	Linux	7	4%
6	Siemens	6	3%
7	EHCP	5	3%
8	Medtronic	3	2%
9	Safe'N'Sec	3	2%

10	其他	66	37%
----	----	----	-----

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，33 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Mikrotik Winbox 任意文件访问漏洞、Google Android LG 组件权限提升漏洞、Siemens SICLOCK TC 产品绕过认证漏洞、Apache Tomcat CORS Filter 安全绕过漏洞、Siemens SICLOCK TC 产品拒绝服务漏洞”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/>

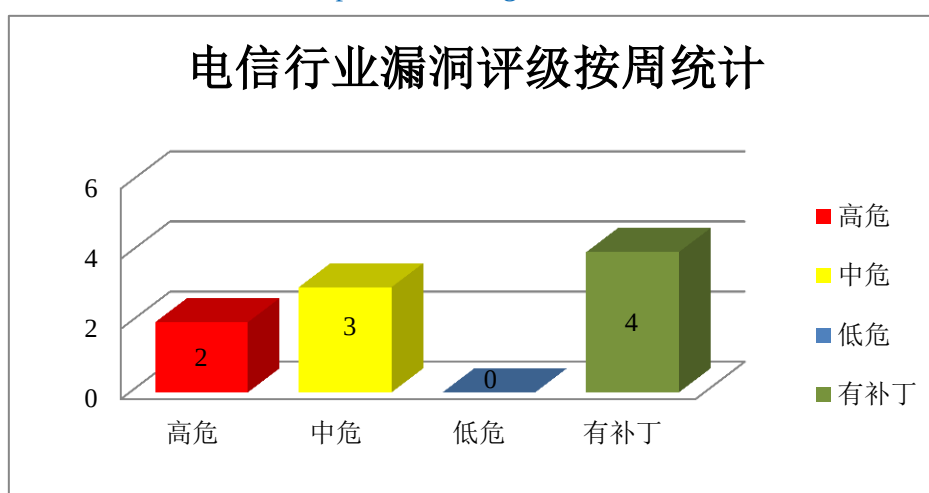


图 3 电信行业漏洞统计

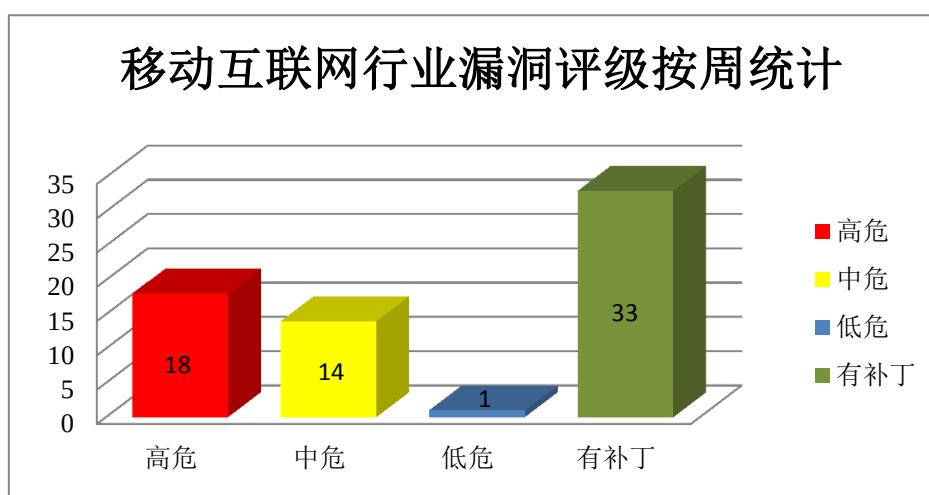


图 4 移动互联网行业漏洞统计

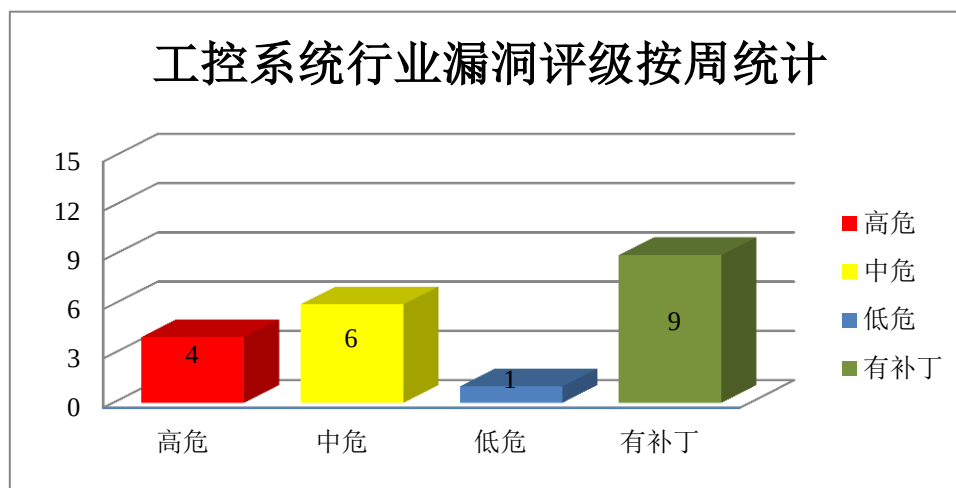


图 5 工控系统行业漏洞统计

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、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 Kernel 组件权限提升漏洞（CNVD-2018-12652）、Google Android NVIDIA 组件权限提升漏洞（CNVD-2018-12654、CNVD-2018-12655）、Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-12656、CNVD-2018-12659、CNVD-2018-12660、CNVD-2018-12661、CNVD-2018-12663）。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-2018-12652>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12654>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12655>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12656>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12659>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12660>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12661>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12663>

2、IBM 产品安全漏洞

IBM Rational Quality Manager 是基于 Web 的合作性质量管理解决方案。IBM Rational Collaborative Lifecycle Management 是应用生命周期管理解决方案。本周，上述产

品被披露存在跨站脚本漏洞，攻击者可利用漏洞允许用户在 Web UI 中嵌入任意 JavaScript 代码，导致泄露受信任会话内的凭证。

CNVD 收录的相关漏洞包括：IBM RQM/RCLM 跨站脚本漏洞（CNVD-2018-12619、CNVD-2018-12620、CNVD-2018-12622、CNVD-2018-12621、CNVD-2018-12623、CNVD-2018-12624、CNVD-2018-12626、CNVD-2018-12627）。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-2018-12619>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12620>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12622>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12621>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12623>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12624>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12626>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12627>

3、Microsoft 产品安全漏洞

Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2016、Windows Server Version 1709 和 Windows Server Version 1803 都是服务器操作系统。Microsoft Office 2010 SP2 等都是办公软件套件产品。Excel 是 Office 套件中的一款电子表格处理软件。Microsoft Office Online Server 2016 是一套基于 Web 的办公软件套件。Office Web Apps Server 2013 SP1 是一款为 Office 文件提供基于浏览器的文件查看和编辑功能的 Office Server 产品。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，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Windows 'HTTP.sys'远程代码执行漏洞、Microsoft Windows DNSAPI 远程代码执行漏洞（CNVD-2018-12562）、Microsoft Windows Hyper-V Code Integrity 权限提升漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2018-12566）、Microsoft Windows 'HTTP.sys'拒绝服务漏洞（CNVD-2018-12567）、Microsoft Windows WebDAV 拒绝服务漏洞、Microsoft Windows Media Foundation 内存破坏漏洞、Microsoft Office 权限提升漏洞（CNVD-2018-12577）。其中，除“Microsoft Windows 'HTTP.sys'拒绝服务漏洞（CNVD-2018-12567）、Microsoft Windows WebDAV 拒绝服务漏洞”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-2018-12561>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12562>
<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12566>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12567>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12573>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12576>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12577>

4、Apache 产品安全漏洞

Apache PDFBox 是一个开源的、基于 Java 并提供创建新的 PDF 文档、修改现有的 PDF 文档等功能的工具库。Apache Zookeeper 是一个软件项目。Apache Tomcat 是一款轻量级 Web 应用服务器。Apache Qpid 是一款面向对象的消息中间件，它是一个 AMQP（高级消息队列协议）的实现，可以和符合 AMQP 协议的系统进行通信，并提供了 C++、Python、Java、C#等编程语言的客户端库。Apache MXNet 是一套可扩展的深度学习框架。Apache HBase 是一套构建在 Apache Hadoop 和 Apache ZooKeeper 上的面向列的分布式数据库。Apache CXF 是一个开源服务框架。Apache Cassandra 是一套开源分布式 NoSQL 数据库系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能限制，获取敏感信息，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：Apache PDFBox's AFMParse 拒绝服务漏洞、Apache ZooKeeper 安全绕过漏洞、Apache Tomcat CORS Filter 安全绕过漏洞、Apache Qpid Broker-J 拒绝服务漏洞（CNVD-2018-12673）、Apache MXNet 信息泄露漏洞、Apache HBase 安全限制绕过漏洞、Apache CXF 拒绝服务漏洞（CNVD-2018-12677）、Apache Cassandra 任意 Java 代码执行漏洞。其中，“Apache Tomcat CORS Filter 安全绕过漏洞、Apache Cassandra 任意 Java 代码执行漏洞”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-2018-12487>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12670>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12671>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12673>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12676>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12678>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2018-12679>

5、Electro Industries GaugeTech Nexus 设备信息泄露漏洞

Electro Industries GaugeTech Nexus devices 是一款具有高级通讯功能的公共事业计费设备。本周，Electro Industries GaugeTech Nexus devices 被披露存在信息泄露漏洞，远程攻击者可通过对 meter_information.htm、diag_system.htm 或 diag_dnp_lan_wan.htm

URI 发送直接请求利用该漏洞获取敏感信息。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-2018-12419>

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-2018-12488	EMC ECS S3 身份验证绕过漏洞	高	用户可联系供应商获得补丁信息： https://www.dellemc.com
CNVD-2018-12501	Siemens SICLOCK TC 产品拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://cert-portal.siemens.com/productcert/pdf/ssa-197012.pdf
CNVD-2018-12547	GLPI SQL 注入漏洞（CNVD-2018-12547）	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/glpi-project/glpi/issues/4270
CNVD-2018-12555	podman 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://github.com/projectatomic/libpod/commit/bae80a0b663925ec751ad2784ca32989403cdc24
CNVD-2018-12713	LilyPond 参数注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=898373
CNVD-2018-12503	Siemens SICLOCK TC 产品未授权操作漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://cert-portal.siemens.com/productcert/pdf/ssa-197012.pdf
CNVD-2018-12539	Micro Focus Secure Messaging Gateway Web administration 组件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，补丁获取链接： https://support.microfocus.com/kb/doc.php?id=7023133
CNVD-2018-12492	EMC RSA Certificate Manager 目录遍历漏洞	高	用户可联系供应商获得补丁信息： http://www.emc.com/
CNVD-2018-12490	Apple SwiftNIO 缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： https://github.com/apple/swift-nio/releases/tag/1.8.0
CNVD-2018-12502	Siemens SICLOCK TC 产品绕过认证漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：

			https://cert-portal.siemens.com/productcert/pdf/ssa-197012.pdf
--	--	--	---

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，IBM、Microsoft、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。另外，Electro Industries GaugeTech Nexus devices 被披露存在信息泄露漏洞，远程攻击者可通过对 meter_information.htm、diag_system.htm 或 diag_dnp_lan_wan.htm URI 发送直接请求利用该漏洞获取敏感信息。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. 微信支付 SDK 被曝 XXE 漏洞，可窃取商家密钥伪造订单

国外一名白帽子发现了微信支付的漏洞，根据白帽子给出的漏洞描述，使用微信支付时，商家需要提供通知网址以接受异步支付结果。问题是微信在 JAVA 版本 SDK 中的实现存在一个 xxe 漏洞。攻击者可以向通知 URL 构建恶意 payload，根据需要窃取商家服务器的任何信息。一旦攻击者获得商家的关键安全密钥（md5-key 和 merchant-Id 等），就可以通过发送伪造信息来欺骗商家购买任何东西而无需付费。

参考链接：<http://www.freebuf.com/news/176407.html>

2. 华为部分产品曝弱加密算法漏洞，可导致信息泄露

近日，华为在一份编号为“huawei-sa-20180703-01-algorithm”的安全通报中指出，某些华为产品存在一个弱加密算法漏洞，成功利用可能会导致信息泄露。根据通报的描述，此漏洞于去年年底被发现。漏洞编号为 HWPSIRT-2017-12135，并且已经获得了 CVE 漏洞编号——CVE-2017-17174。CVSSv3 评分 5.3，属于一个中等风险漏洞，这来源于它的成功利用并不容易实现。华为解释说，要利用此漏洞，远程未经身份验证的攻击者必须捕获客户端与受影响产品之间的 TLS 流量。攻击者可能会对 RSA 密钥交换启动 Bleichenbacher 攻击，以通过某些密码分析操作解密会话密钥和先前捕获的会话。当然，成功的利用便会导致在上述中提到的信息泄露。

参考链接：<https://www.easyaq.com/news/45530704.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