国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 8 月 13 日-2018 年 8 月 19 日　　2018 年第 33 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 274 个，其中高危漏洞 107 个、中危漏洞 155 个、低危漏洞 12 个。漏洞平均分值为 6.24。本周收录的漏洞中，涉及 0day 漏洞 71 个（占 26%），其中互联网上出现“NEWMARK NMCMS SQL 注入漏洞、EMLsoft 'numPerPage'参数 SQL 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 942 个，与上周（893 个）环比增长 5%。

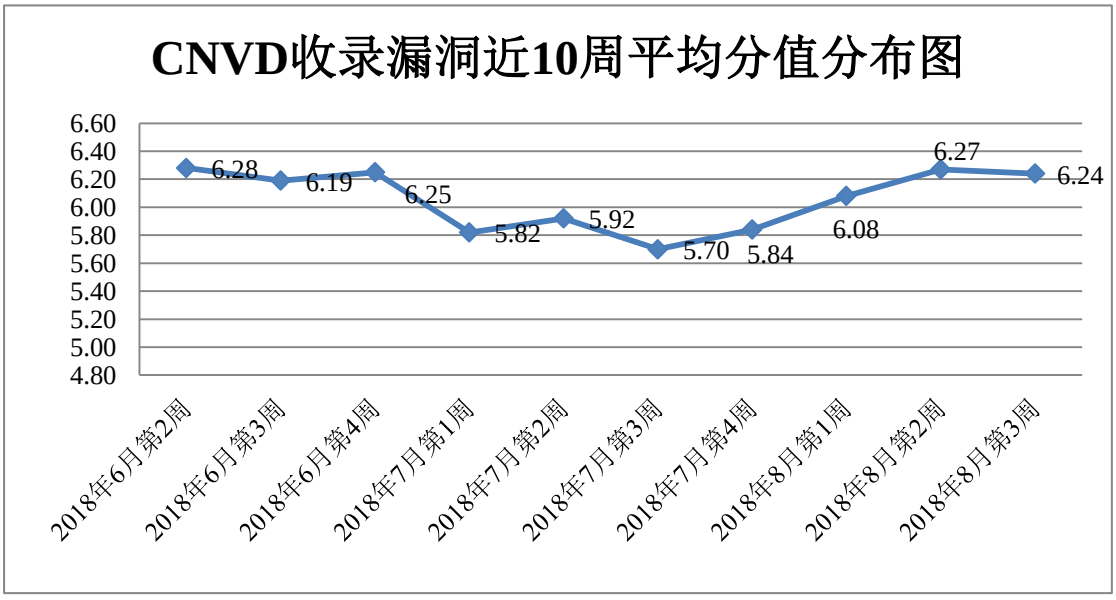

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北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、深圳市深信服电子科技有限公司、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。山东云天安全技术有限公司、任子行网络技术股份有限公司、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）、上海银基信息安全技术股份有限公司、河南信安世纪科技有限公司、国家互联网应急中心研究所，北京同余科技有限公司、北京禹宏信安科技有限公司、北京智游网安科技有限公司、杭州海康威视数字技术股份有限公司、海南神州希望网络有限公司、河北网信智安信息技术有限公司及其他个人白帽子向 CNVD 提交了 942 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 491 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
漏洞盒子	320	320
哈尔滨安天科技股份有限公司	201	0
360 网神（补天平台）	171	171
北京天融信网络安全技术有限公司	164	10
华为技术有限公司	122	122
深圳市深信服电子科技有限公司	95	3
新华三技术有限公司	94	0
北京神州绿盟科技有限公司	57	14
中国电信集团系统集成有限责任公司	57	0
恒安嘉新(北京)科技股份公司	39	0
北京无声信息技术有限公司	31	29
北京知道创宇信息技术有限公司	16	15
沈阳东软系统集成工程有限公司	6	6
厦门服云信息科技有限公司	5	0
山东云天安全技术有限公司	45	45

任子行网络技术股份有限公司	10	10
中新网络信息安全股份有限公司	7	7
四川虹微技术有限公司（子午攻防实验室）	3	3
上海银基信息安全技术股份有限公司	3	3
河南信安世纪科技有限公司	3	3
国家互联网应急中心研究所，北京同余科技有限公司	3	3
北京禹宏信安科技有限公司	1	1
北京智游网安科技有限公司	1	1
杭州海康威视数字技术股份有限公司	1	1
海南神州希望网络有限公司	1	1
河北网信智安信息技术有限公司	1	1
CNCERT 吉林分中心	6	6
CNCERT 甘肃分中心	3	3
CNCERT 新疆分中心	3	3
CNCERT 河南分中心	2	2
CNCERT 天津分中心	2	2
CNCERT 浙江分中心	1	1
CNCERT 广东分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	154	154
报送总计	1630	942

本周漏洞按类型和厂商统计

本周，CNVD 收录了 213 个漏洞。应用程序漏洞 150 个，WEB 应用漏洞 95 个，网络设备漏洞 17 个，操作系统漏洞 6 个，安全产品漏洞 4 个，数据库漏洞 2 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	150
WEB 应用漏洞	95
网络设备漏洞	17
操作系统漏洞	6
安全产品漏洞	4
数据库漏洞	2

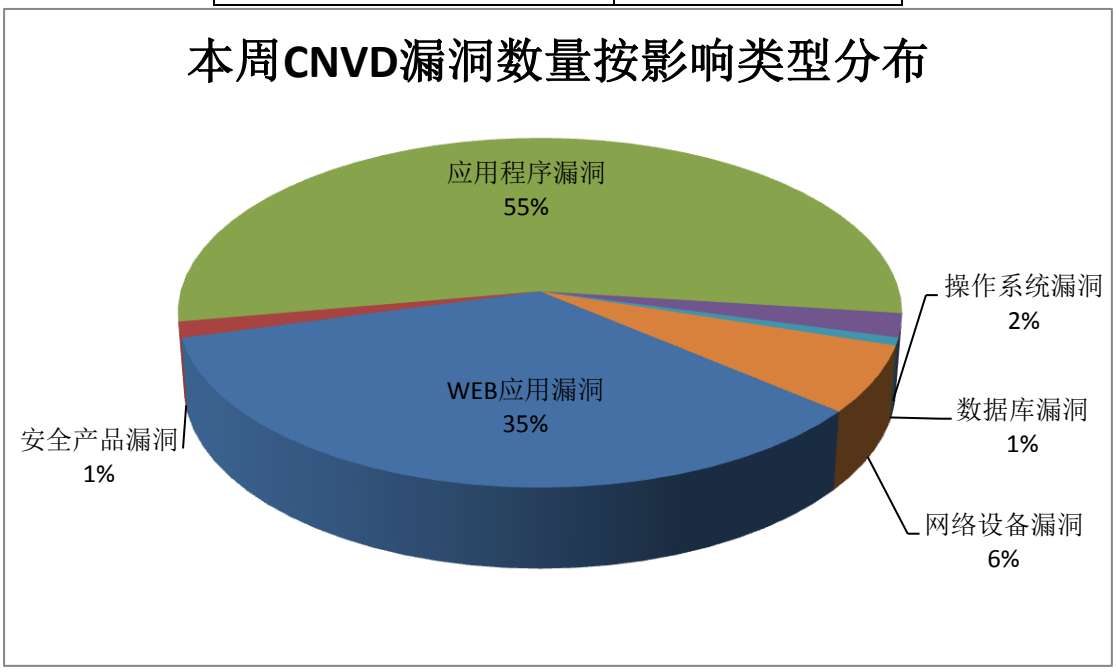

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Intel、Apache 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	22	8%
2	Intel	21	8%
3	Apache	13	4%
4	SAP	13	4%
5	Libgig	11	4%
6	Cybozu	10	4%

7	BaserCMS	7	3%
8	Joomla	7	3%
9	WordPress	7	3%
10	其他	163	59%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，15 个移动互联网行业漏洞（如下图所示）。其中，“D-Link DIR-815 访问限制绕过漏洞、Huawei 1288H 和 2288H 机架服务器 JSON 注入漏洞、Oracle Database Server Java VM 组件远程漏洞、AppCMS 后台模板管理处存在命令执行漏洞、Citrix XenMobile Server XML 外部实体处理漏洞”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/

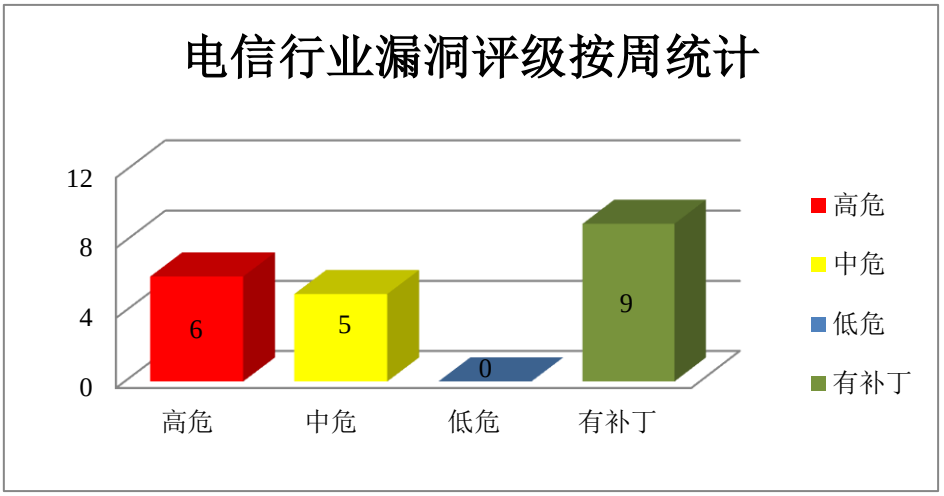

图 3 电信行业漏洞统计

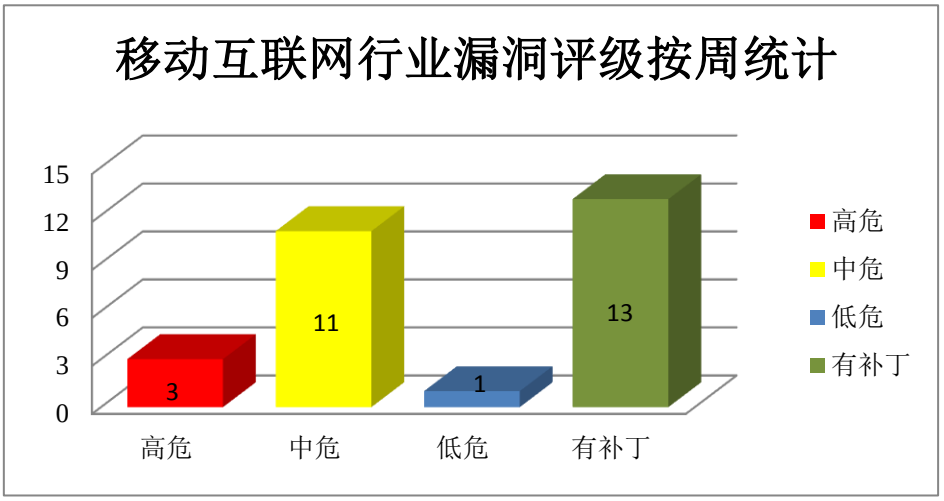

图 4 移动互联网行业漏洞统计

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 产品安全漏洞

Microsoft Exchange Server 是一套电子邮件服务程序，它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。Microsoft Windows 7 等都是一系列操作系统。Windows FTP Server 是其中的一个 FTP（文件传输协议）服务器。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发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server 内存破坏漏洞、Microsoft Internet Explorer 和 Edge 脚本引擎内存破坏漏洞（CNVD-2018-15434、CNVD-2018-15435、CNVD-2018-15436）、Microsoft Internet Explorer 脚本引擎内存破坏漏洞（CNVD-2018-15439、CNVD-2018-15438）、Microsoft Visual Studio 远程代码执行漏洞、Microsoft Windows FTP Server 拒绝服务漏洞。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-2018-15416

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15434

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15435

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15436

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15439

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15438

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15446

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15447

2、Intel 产品安全漏洞

Intel Quartus II 是一套用于硬件编程的软件。Intel Server Board 是一款服务器主板。Compute Module 是一款计算模块。Server System 是一款服务器阵列卡。Intel 4th Gen Intel Core Processor 等都是不同系列的中央处理器（CPU）产品。Intel Processor Diagnostic Tool（IPDT）是一款处理器功能诊断工具。Intel Converged Security Manageability Engine 是一款使用在 CPU（中央处理器）中的安全管理引擎。Active Management Technology（AMT）是其中的一个主动管理组件。Intel Saffron MemoryBase 是一款用于 Saffron 的内存基础套件。本周，上述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，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Intel Quartus II 权限提升漏洞、Intel Server Board、Compute Module 和 Server System 拒绝服务漏洞、多款 Intel 产品信息泄露漏洞、Intel Processor Diagnostic Tool 权限提升漏洞（CNVD-2018-15596、CNVD-2018-15597）、Intel Converged Security Manageability Engine Active Management Technology 权限提升漏洞、Intel Saffron MemoryBase 权限提升漏洞（CNVD-2018-15599、CNVD-2018-15600）。其中，除“Intel Quartus II 权限提升漏洞、多款 Intel 产品信息泄露漏洞、Intel Saffron MemoryBase 权限提升漏洞”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-2018-15553

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15554

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15594

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15596

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15597

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15598

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15599

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15600

3、Apache 产品安全漏洞

Apache Camel 是一套开源的基于 Enterprise Integration Pattern(企业整合模式，简称 EIP)的集成框架。Apache Ignite 是一套用于大规模的数据集处理的内存计算和事务管理平台。Apache Kafka 是一个开源的分布式流媒体平台。Apache Storm 是一个免费开源的分布式实时计算系统。Apache Tomcat 是一款轻量级 Web 应用服务器，它主要用于开发和调试 JSP 程序，适用于中小型系统。Apache Ant 是一套用于 Java 软件开发的自动化工具。该工具主要用于软件的编译、测试和部署等。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件，绕过安全限制，执行未授权的操作，执行任意代码等。

CNVD 收录的相关漏洞包括：Apache Camel Core XSD validation processor 外部实体信息泄露漏洞、Apache Ignite 任意代码执行漏洞（CNVD-2018-15540）、Apache Kafka 安全绕过漏洞、Apache Storm 任意代码执行漏洞（CNVD-2018-15544）、Apache Tomcat 安全限制绕过漏洞（CNVD-2018-15543）、Apache Ant 未授权操作漏洞、Apache Tomcat Native 身份验证漏洞（CNVD-2018-15545、CNVD-2018-15547）。其中，“Apache Ignite 任意代码执行漏洞（CNVD-2018-15540）、Apache Storm 任意代码执行漏洞（CNVD-2018-15544）”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-2018-15538

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15540

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15539

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15544

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15543

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15546

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15545

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15547

4、SAP 产品安全漏洞

SAP Internet Graphics Server（IGS）是一款图形服务器。SAP MaxDB 是一套跨平台的、兼容 ANSI SQL-92 的关系数据库管理系统。SAP Identity Management 是一套能够嵌入到业务流程中的身份管理应用程序。SAP HANA 是一套实时数据分析平台。SAP NetWeaver 是一套面向服务的集成化应用平台，该平台可为 SAP 应用提供开发和运行环境。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，执行任意代码，绕过某些安全限制并执行未授权的操作。

CNVD 收录的相关漏洞包括：SAP Internet Graphics Server Portwatcher 拒绝服务漏洞（CNVD-2018-15390）、SAP MaxDB ODBC 远程代码注入漏洞、SAP Internet Graphics Server Portwatcher 拒绝服务漏洞、SAP Identity Management XML 外部实体注入漏洞 、SAP Identity Management 信息泄露漏洞、SAP Internet Graphics Server HTTP 和 RFC listener 拒绝服务漏洞、SAP HANA SAP Systems Installation 权限提升漏洞、SAP NetWeaver AS Java Log Injection 安全绕过漏洞。其中，“SAP MaxDB ODBC 远程代码注入漏洞、SAP HANA SAP Systems Installation 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-2018-15390

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15395

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15394

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15397

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15396

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15402

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15509

http://www.cnvd.org.cn/flaw/show/CNVD-2018-15507

5、PbootCMS 'scode'参数 SQL 注入漏洞

PbootCMS 是一款使用 PHP 语言开发的开源企业建站内容管理系统（CMS）。本周，PbootCMS 被披露存在 SQL 注入漏洞。远程攻击者可通过向\apps\home\controller\ParserController.php 脚本发送'scode'参数利用该漏洞从数据库中获取重要信息。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-2018-15191

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-2018-15251	Citrix XenMobile Server 未认证文件上传漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.citrix.com/article/CTX234879
CNVD-2018-15256	Jenkins Global Build Stats 插件存在多个漏洞（CNVD-2018-15256）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://jenkins.io/security/advisory/2017-10-23/
CNVD-2018-15262	Syntastic 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/vim-syntastic/syntastic/commit/6d7c0b394e001233dd09ec473fbea2002c72632f
CNVD-2018-15260	WordPress WP Live Chat Support Pro 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://wordpress.org/plugins/wp-live-chat-support/#developers
CNVD-2018-15268	Quest KACE System Management Appliance SQL 注入漏洞（CNVD-2018-15268）	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.quest.com/download-install-detail/6086148
CNVD-2018-15389	Huawei 1288H 和 2288H 机架服务器 JSON 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180523-01-json-en
CNVD-2018-15392	SeedDMS SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/seeddms/code/ci/seeddms-5.1.x/tree/CHANGELOG
CNVD-2018-15401	Trend Micro Smart Protection Server SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://success.trendmicro.com/solution/1119715
CNVD-2018-15400	Cybozu Garoon Notifications 应用程序 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://kb.cybozu.support/article/33120/
CNVD-2018-15413	D-Link DIR-815 访问限制绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：ftp://ftp2.dlink.com/SECURITY_ADVISEMENTS/DIR-815/REVB/DIR-815_REVB_FIRMWARE_PATCH_NOTES_2.07.B01_EN.PDF

小结：本周，Microsoft 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，Intel、Apache、SAP 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，绕过安全限制，执行未授权的操作，执行任意代码或发起拒绝服务攻击等。另外，PbootCMS 被披露存在 SQL 注入漏洞。远程攻击者可通过向\apps\home\controller\ParserController.php 脚本发送'scode'参数利用该漏洞从数据库中获取重要信息。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、EMLsoft 'numPerPage'参数 SQL 注入漏洞

验证描述

EMLsoft 是一套企业通讯录管理系统。

EMLsoft 5.4.5 版本中的 upload\eml\action\action.address.php 文件存在 SQL 注入漏洞。远程攻击者可借助'numPerPage'参数利用该漏洞查看、添加、修改或删除后端数据库中的信息。

验证信息

POC 链接：https://www.exploit-db.com/exploits/44911/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-15411

信息提供者

哈尔滨安天科技股份有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 英特尔 CPU 新漏洞“预兆”（L1TF）

近期，英特尔 CPU 再曝三个新漏洞（CVE-2018-3615、CVE-2018-3620 和 CVE-20

18-3646），被称为“预兆”（L1TF）。“预兆”是“幽灵”和“熔断”漏洞的衍生变种。受影响的处理器包括 Intel Core i3/i5/i7/M 处理器(45nm/32nm)、Intel Xeon 3400/3600/5500/5600/6500/ 7500 系列等。英特尔现已发布补丁。

参考链接：https://www.easyaq.com/news/1944379123.shtml

2. 微软 Cortana 出现漏洞，即使系统锁定也能使用浏览功能

近日，安全研究专家对外表示，Cortana 被曝存在安全缺陷。如果你的 Windows 电脑开启了锁屏启动微软 Cortana 数字助手的话，意味着攻击者将能够窃取你存储在浏览器缓存中的用户凭证。

参考链接：http://www.freebuf.com/news/181256.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：010-82991537