国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 03 月 18 日-2019 年 03 月 24 日　　2019 年第 12 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 196 个，其中高危漏洞 54 个、中危漏洞 114 个、低危漏洞 28 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 62%），其中互联网上出现“LayerBB SQL 注入漏洞、ThinkCMF SQL 注入漏洞（CNVD-2019-07961）”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 1788 个，与上周（1675 个）环比增长 7%。

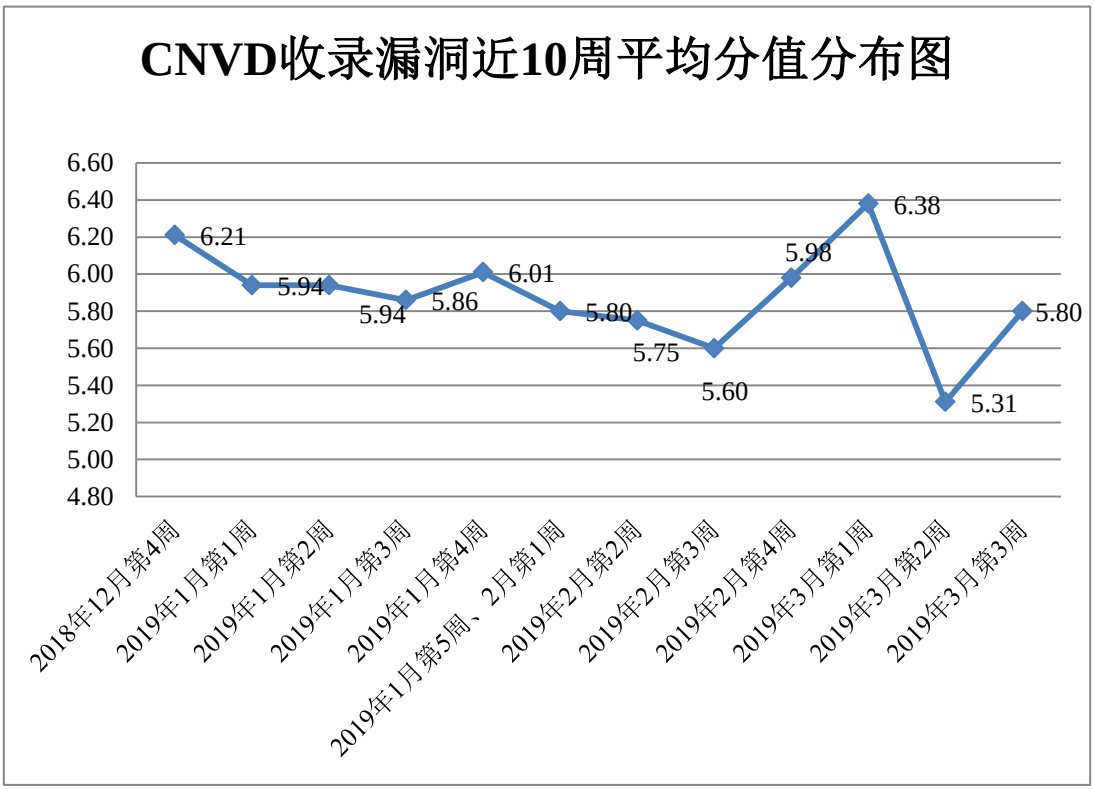

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 9 起，向银行、保险、能源等重要行业单位通报漏洞事件 25 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 334 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 37 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

广州网软志成信息科技有限公司、肆方網路科技有限公司、西门子（中国）有限公司、广州永拓信息科技有限公司、哈尔滨风腾电子商务有限公司、浦江迅杰网络科技有限公司、兰州天杰网络科技有限公司、重庆然宇网络科技有限公司、邳州天目网络科技有限公司、漳州市芗城帝兴软件开发有限公司、宁波高新区奥凯网络科技有限公司、台州精迅信息技术有限公司、深圳市亿天联科技有限公司、北京因酷时代科技有限公司、江西金磊科技发展有限公司、深圳市海洋蓝科技有限公司、金华市宁志网络科技有限公司、海南赞赞网络科技有限公司、上海商派网络科技有限公司、灵宝简好网络科技有限公司、广东凯格网络科技有限公司、广州巨腾信息科技有限公司、合众商道（大连）科技有限公司、泰州智搜网络科技有限公司、淇晨科技公司、天天 asp 开发网、企业第一网、米酷资源网、MyfCMS-闵益飞内容管理系统、EOVA 简单开发社区、信呼、鲶鱼 CMS、至诚软件工作室、棠下互联、企炬中国、SeaCMS、Joomla!、Emerson、iCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、中国电信集团系统集成有限责任公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。中新网络信息安全股份有限公司、山东九州信泰信息科技股份有限公司、国瑞数码零点实验室、北京长亭科技有限公司、安徽锋刃信息科技有限公司、北京圣博润高新技术股份有限公司、重庆贝特计算机系统工程有限公司、山东华鲁科技发展股份有限公司、长春嘉诚信息技术股份有限公司、北京国舜科技股份有限公司、广州竞远安全技术股份有限公司、内蒙古奥创科技有限公司、山东云天安全技术有限公司、山石网科通信技术股份有限公司、安徽长泰信息安全服务有限公司及其他个人白帽子向 CNVD 提交了 1788 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1285 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
斗象科技（漏洞盒子）	839	839

360 网神（补天平台）	446	446
哈尔滨安天科技集团股份有限公司	150	0
北京天融信网络安全技术有限公司	109	7
北京神州绿盟科技有限公司	105	0
中国电信集团系统集成有限责任公司	104	0
华为技术有限公司	78	0
新华三技术有限公司	73	0
北京启明星辰信息安全技术有限公司	63	8
北京数字观星科技有限公司	61	0
深信服科技股份有限公司	39	0
恒安嘉新(北京)科技股份公司	23	0
厦门服云信息科技有限公司	20	0
四川无声信息技术有限公司	12	12
北京知道创宇信息技术有限公司	6	6
西安四叶草信息技术有限公司	1	1
中新网络信息安全股份有限公司	66	66
山东九州信泰信息科技股份有限公司	53	53
国瑞数码零点实验室	46	46
北京长亭科技有限公司	35	35
安徽锋刃信息科技有限公司	31	31
北京圣博润高新技术股份有限公司	17	17
重庆贝特计算机系统工程有限公司	15	15

山东华鲁科技发展股份有限公司	7	7
长春嘉诚信息技术股份有限公司	7	7
北京国舜科技股份有限公司	3	3
广州竞远安全技术股份有限公司	3	3
内蒙古奥创科技有限公司	2	2
山东云天安全技术有限公司	2	2
山石网科通信技术股份有限公司	1	1
安徽长泰信息安全服务有限公司	1	1
浙江分中心	6	6
广西分中心	4	4
北京分中心	2	2
河北分中心	2	2
海南分中心	1	1
河南分中心	1	1
内蒙古分中心	1	1
宁夏分中心	1	1
个人	162	162
报送总计	2598	1788

本周漏洞按类型和厂商统计

本周，CNVD 收录了 196 个漏洞。应用程序漏洞 101 个，WEB 应用漏洞 66 个，网络设备漏洞 22 个，操作系统漏洞 5 个，安全产品漏洞 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	101

WEB 应用漏洞	66
网络设备漏洞	22
数据库漏洞	5
操作系统漏洞	2

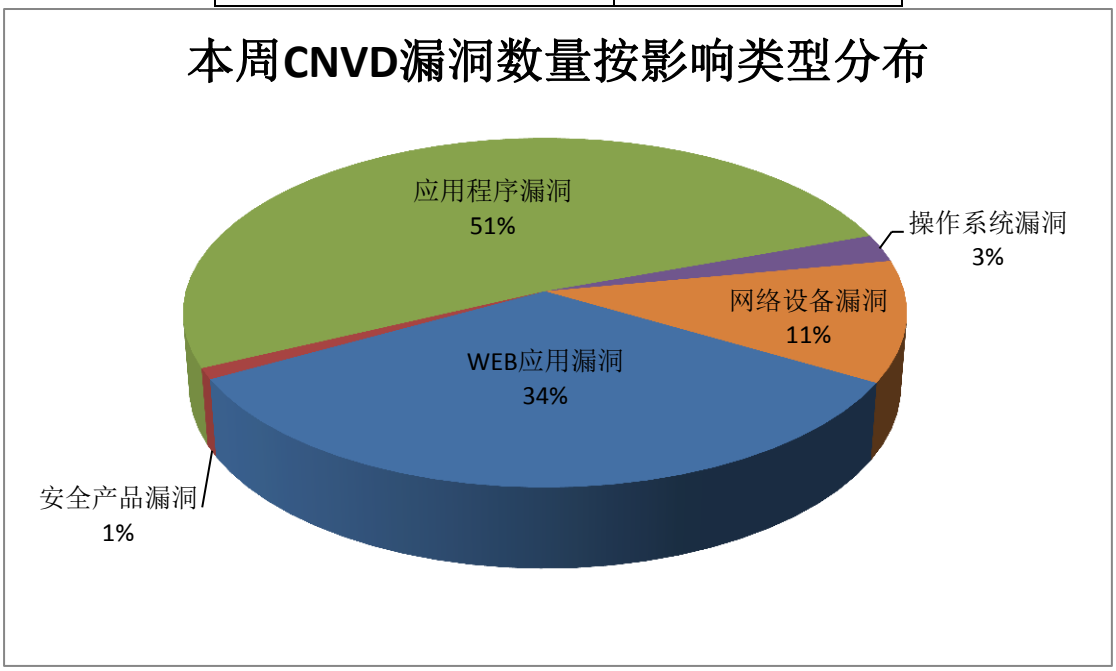

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、DomainMOD、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	WordPress	12	6%
2	DomainMOD	11	6%
3	Microsoft	9	5%
4	Google	9	5%
5	libssh2	8	4%
6	Xen	7	3%
7	Siemens	6	3%
8	FAAD2	6	3%
9	Rdesktop	6	3%
10	其他	122	62%

本周行业漏洞收录情况

本周，CNVD 收录了 6 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，“Google Android Framework 权限提升漏洞、Google Android NVIDIA 组件权限提升漏洞”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/

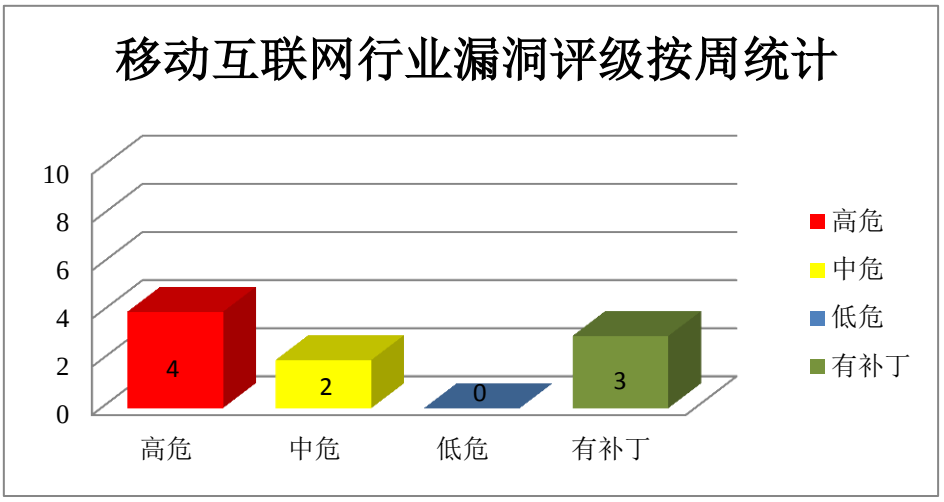

图 3 移动互联网行业漏洞统计

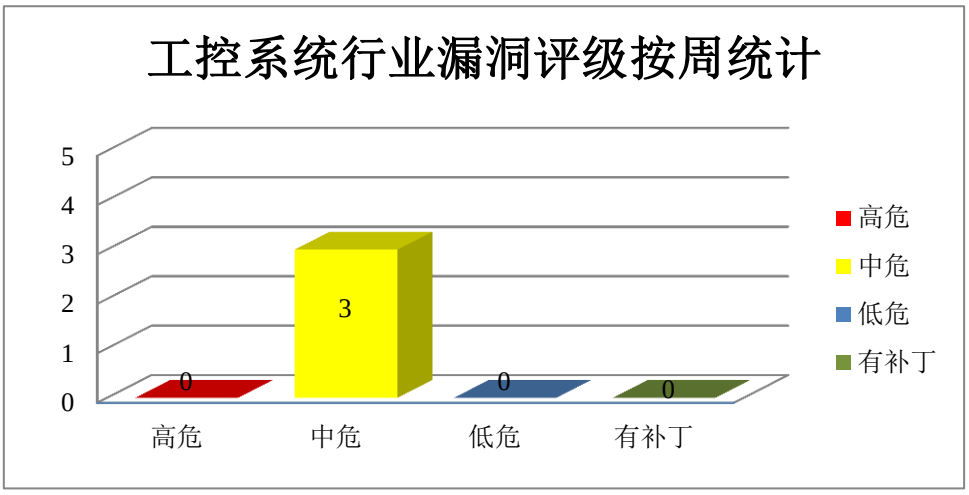

图 4 工控系统行业漏洞统计

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

Google Chrome 是一款 Web 浏览器。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，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 不可信输入验证漏洞、Google Chrome for android 信息泄露漏洞、Google Chrome SVG 对象类型混淆漏洞、Google Android Framework 权限提升漏洞、Google Chrome 命令执行漏洞、Google Android NVIDIA 组件权限提升漏洞、Google Chrome QUIC 网络实现错误漏洞、Google Chrome V8 负 0 错误处理漏洞。其中，“Google Android Framework 权限提升漏洞、Google Android NVIDIA 组件权限提升漏洞”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-2019-07978

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07979

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07980

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07981

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07982

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07984

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07985

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07986

2、Microsoft 产品安全漏洞

Windows 是美国微软公司研发的一套操作系统，Windows 采用了图形化模式 GUI。Windows Subsystem for Linux（简称 WSL）是一个为在 Windows 10 和 Windows Server 2019 上能够原生运行 Linux 二进制可执行文件（ELF 格式）的兼容层。Edge 是微软为 Windows 10 打造的浏览器。Microsoft Office 是一款办公软件套件产品。Microsoft SharePoint 是一套企业业务协作平台。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跨站脚本攻击，获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2019-07383、CNVD-2019-07384、CNVD-2019-07386、CNVD-2019-07385、CNVD-2019-07387）、Microsoft Windows Kernel 信息泄露漏洞、Microsoft Office Access Connectivity Engine 远程代码执行漏洞、Microsoft Office SharePoint 跨站脚本漏洞。其中，除“Microsoft Windows Kernel 信息泄露漏洞、Microsoft Office SharePoint 跨站脚本漏洞”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-2019-07383

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07384

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07386

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07385

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07387

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07974

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07976

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07977

3、libssh2 产品安全漏洞

libssh2 是一款实现 SSH2 协议的客户端 C 库，它能够执行远程命令、文件传输，同时为远程的程序提供安全的传输通道。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务或读取客户端内存中的数据，在客户端系统上执行代码。

CNVD 收录的相关漏洞包括：libssh2 整数溢出漏洞（CNVD-2019-07796、CNVD-2019-07798、CNVD-2019-07799、CNVD-2019-07797、CNVD-2019-07800、CNVD-2019-07801、CNVD-2019-07802、CNVD-2019-07803）。其中，“libssh2 整数溢出漏洞（CNVD-2019-07796、CNVD-2019-07798、CNVD-2019-07799）”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-2019-07796

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07797

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07798

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07799

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07800

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07801

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07802

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07803

4、WordPress 产品安全漏洞

WordPress 是一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，该产品被披露存在打开重定向漏洞，攻击者可利用漏洞进行网络钓鱼诈骗并窃取用户凭据。

CNVD 收录的相关漏洞包括：WordPress UsaMusic-PC Themes 打开重定向漏洞、WordPress Concise Themes 打开重定向漏洞、WordPress 2018110612035976 Themes 打开重定向漏洞、WordPress BigChrome Themes 打开重定向漏洞、WordPress Zangai Themes 打开重定向漏洞、WordPress Wngzs Themes 打开重定向漏洞、WordPress itiis Themes 打开重定向漏洞、WordPress fxPro.Cn Themes 打开重定向漏洞。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布该漏洞的修补程序。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-2019-07450

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07451

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07549

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07550

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07551

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07557

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07554

http://www.cnvd.org.cn/flaw/show/CNVD-2019-07555

5、LayerBB SQL 注入漏洞

LayerBB 是一套小型论坛软件。本周，LayerBB 被披露存在 SQL 注入漏洞。远程攻击者可通过向 search.php 文件发送‘search_query’参数利用该漏洞执行 SQL 命令。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-2019-07937

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-2019-07448	Zimbra 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.zimbra.com/
CNVD-2019-07542	CapMon Access Manager 访问控制错误漏洞（CNVD-2019-07542）	高	目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://capmon.dk/
CNVD-2019-07786	Columbia Weather Systems Weather MicroServer 输入验证漏洞	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://columbiaweather.com/
CNVD-2019-07787	Columbia Weather Systems Weather MicroServer 代码注入漏洞	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://columbiaweather.com/
CNVD-2019-07788	Columbia Weather Systems Weather MicroServer 未授权访问漏洞	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://columbiaweather.com/
CNVD-2019-07807	rdesktop 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://github.com/rdesktop/rdesktop/commit/4dca546d04321a610c1835010b5dad85163b65e1
CNVD-2019-07809	rdesktop 整数溢出漏洞（CNVD-2019-07809）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/rdesktop/rdesktop/commit/4dca546d04321a610c1835010b5d

			ad85163b65e1
CNVD-2019-07887	Five9 Agent Desktop Plus 访问控制错误漏洞	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.five9.com/
CNVD-2019-07932	UltraVNC 缓冲区溢出漏洞	高	目前厂商已发布新版本，以修复此安全问题，详情请关注厂商主页：https://www.uvnc.com/
CNVD-2019-07944	Xen 影式分页冲突漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://xenbits.xen.org/xsa/advisory-280.html

小结：本周，Google 被披露存在存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码等。此外，Microsoft、libssh2、WordPress 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行跨站脚本攻击，获取敏感信息，造成拒绝服务或读取客户端内存中的数据，执行任意代码等。另外，EmpireCMS 被披露存在跨站请求伪造漏洞。远程攻击者可利用该漏洞添加用户账户。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、LayerBB SQL 注入漏洞

验证描述

LayerBB 是一套小型论坛软件。

LayerBB 1.1.1 版本中存在 SQL 注入漏洞。远程攻击者可通过向 search.php 文件发送‘search_query’参数利用该漏洞执行 SQL 命令。

验证信息

POC 链接：https://www.exploit-db.com/exploits/45530

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-07937

信息提供者

华为技术有限公司

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. Norsk Hydro 遭勒索攻击，多个工厂 IT 系统崩溃

铝制造商之一 Norsk Hydro（挪威海德鲁公司）位于欧美的多个工厂运营遭受“大规模的网络攻击”，导致 IT 系统无法使用，因此不得不关闭。Norsk Hydro 公司发布新闻稿称，该公司临时关闭多个工厂并将挪威、卡塔尔和巴西等国家的工厂运营模式改为“可以使用的”手动运营模式，以继续执行某些运营。这次网络攻击始于美国，是由该公司的 IT 专家在周一晚上晚些时候（欧洲中部时间）首先检测到的，目前该公司正在缓解攻击并调查了解攻击的蔓延程度。该公司表示，“Hydro 的优先任务是继续确保安全操作并降低运营和金融影响。该问题并未导致任何与安全相关的事件发生。”

参考链接：https://www.secrss.com/articles/9230

2. 谷歌白帽子发现 Windows 系统全新漏洞门类

Google Project Zero 白帽研究员 James Forshaw 发现位于 Windows kernel 模式驱动中的漏洞，利用该漏洞可以进行权限提升。该漏洞是由于处理特定请求时缺乏必要检查导致的。Windows 使用 PreviousMode 域来设置 UserMode 或 KernelMode，然后确定调用的参数是否来源于可信源。该机制也用于文件创建和打开，kernel 模式代码可以从不同的 API 函数中选择，包括到 I/O 管理器内部函数 IopCreateFile 的函数。在这种情况下，PreviousMode 会被分配一个特定的变量来确定是否检查有效的参数和缓存。操作系统使用该变量进行设备对象的检查，即是否是 UserMode。IopCreateFile 中的 Options 参数会暴露给一些 API 函数，这些 API 函数只能从 kernel 模式来调用以设定覆盖 AccessMode 的 flag，并设置为 KernelMode。

参考链接：https://securityaffairs.co/wordpress/82642/hacking/windows-privilege-escalation-bug-class.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