国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 1 月 1 日-2018 年 1 月 7 日 **2018 年第 1 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**高**。

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 219 个，其中高危漏洞 63 个、中危漏洞 144 个、低危漏洞 12 个。漏洞平均分值为 6.02。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 23%），其中互联网上出现“Western Digital My Cloud NAS 设备命令注入漏洞、PHP Scripts Mall PHP Multivendor Ecommerce SQL 注入漏洞（CNVD-2018-00078）”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 483 个，与上周（610 个）环比减少 21%。

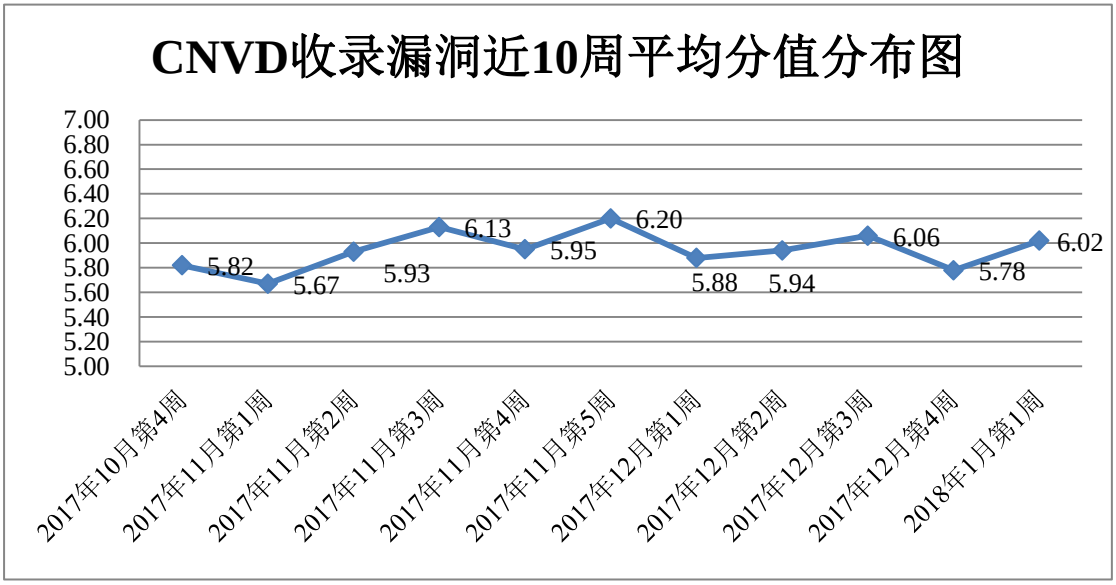

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 29 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 175 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 48 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 22 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：

航天信息股份有限公司、深圳市中兴视通科技有限公司、联想天工网络（深圳）有限公司、北京力控元通科技有限公司、北京中科网威信息技术有限公司、长城宽带网络服务有限公司、北京两面网络科技有限公司、上海长城宽带网络服务有限公司、深圳市锟铻科技有限公司、大庆紫金桥软件技术有限公司、深圳市英威腾电气股份有限公司、中国大唐集团公司、北京五岳鑫信息技术股份有限公司、福建讯盟软件有限公司、北京亚控科技发展有限公司、信呼办公软件、慧星网络科技工作室、Tibbo Technology、行云海 CMS。

本周，CNVD 发布了《关于 Western Digital My Cloud NAS 设备存在高危漏洞的安全公告》、《关于 CPU 处理器内核存在 Meltdown 和 Spectre 漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4357

http://www.cnvd.org.cn/webinfo/show/4359

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天融信、H3C、安天实验室、华为技术有限公司、恒安嘉新等单位报送数量较多。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、山石网科通信技术有限公司、福建榕基软件股份有限公司、广州万方计算机科技有限公司、杭州默安科技有限公司及其他个人白帽子向 CNVD 提交了 483 个以事件型漏洞为主的原创漏洞。

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
天融信	377	0
H3C	194	0
安天实验室	180	0
360 网神	149	149
华为技术有限公司	146	0
漏洞盒子	142	142

恒安嘉新	95	0
绿盟科技	62	0
启明星辰	60	0
中国电信集团系统集成有限责任公司	29	0
卫士通信息产业股份有限公司	25	0
杭州安恒信息技术有限公司	20	0
知道创宇	2	0
四川虹微技术有限公司（子午攻防实验室）	26	26
南京联成科技发展股份有限公司	22	22
中新网络信息安全股份有限公司	6	6
山石网科通信技术有限公司	1	1
福建榕基软件股份有限公司	1	1
广州万方计算机科技有限公司	1	1
杭州默安科技有限公司	1	1
CNCERT 浙江分中心	4	4
CNCERT 宁夏分中心	3	3
CNCERT 上海分中心	3	3
CNCERT 海南分中心	1	1
CNCERT 云南分中心	1	1
CNCERT 广东分中心	1	1
个人	121	121
报送总计	1673	483

本周漏洞按类型和厂商统计

本周，CNVD 收录了 219 个漏洞。其中应用程序漏洞 131 个，web 应用漏洞 34 个，操作系统漏洞 31 个，网络设备漏洞 20 个，安全产品漏洞 2 个，数据库漏洞 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	131
web 应用漏洞	34
操作系统漏洞	31
网络设备漏洞	20
安全产品漏洞	2
数据库漏洞	1

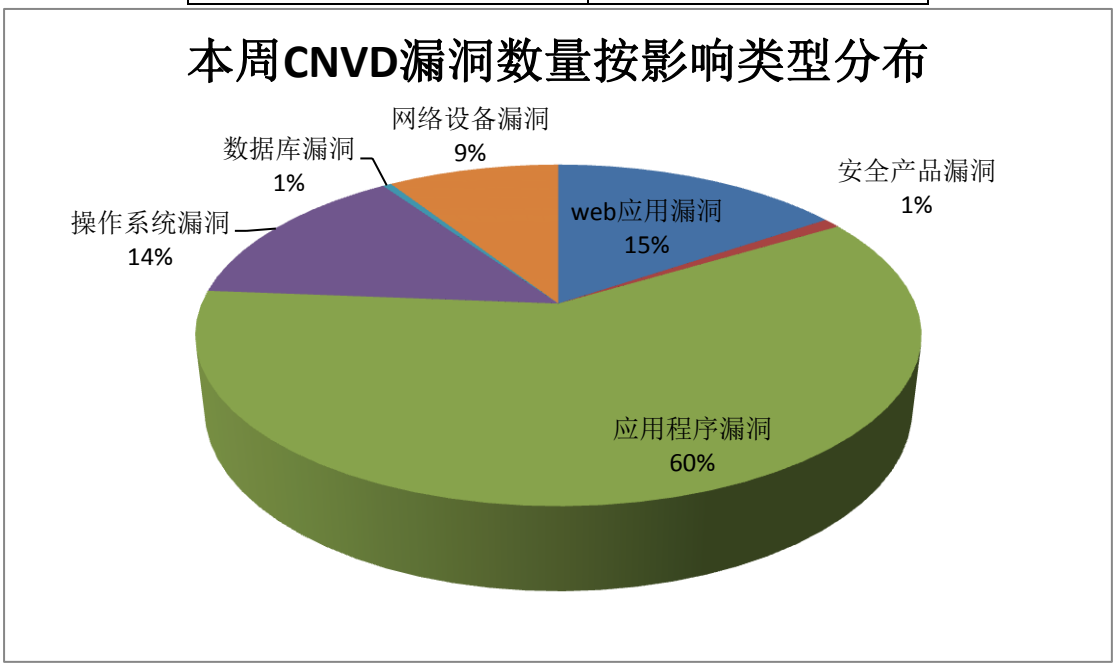

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、Huawei、WordPress 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	Foxit	39	18%
2	Huawei	14	6%
3	WordPress	14	6%
4	Apple	14	6%
5	ImageMagick	11	5%
6	PHP Scripts Mall	10	5%

7	Microsoft	9	4%
8	Western Digital	6	3%
9	Linux	5	2%
10	其他	97	45%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，18 个移动互联网行业漏洞（如下图所示）。其中，“D-Link DSL-6850U 路由器远程命令执行漏洞、Huawei S7700 和 S9700 拒绝服务漏洞、Google Android telephony 提权漏洞、Haystack Arq for Mac helper app 权限提升漏洞、Apple iOS 和 macOS High Sierra IOKit 组件内存破坏漏洞”等漏洞的综合评级为“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/

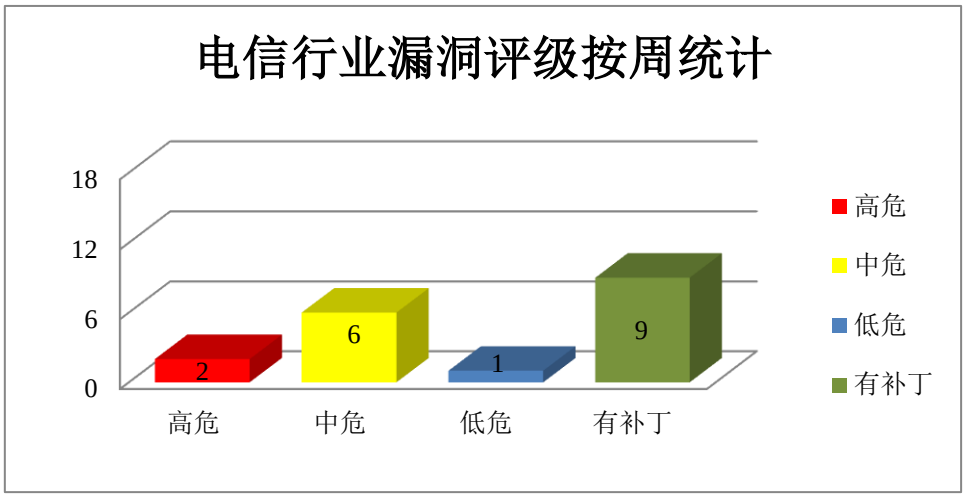

图 3 电信行业漏洞统计

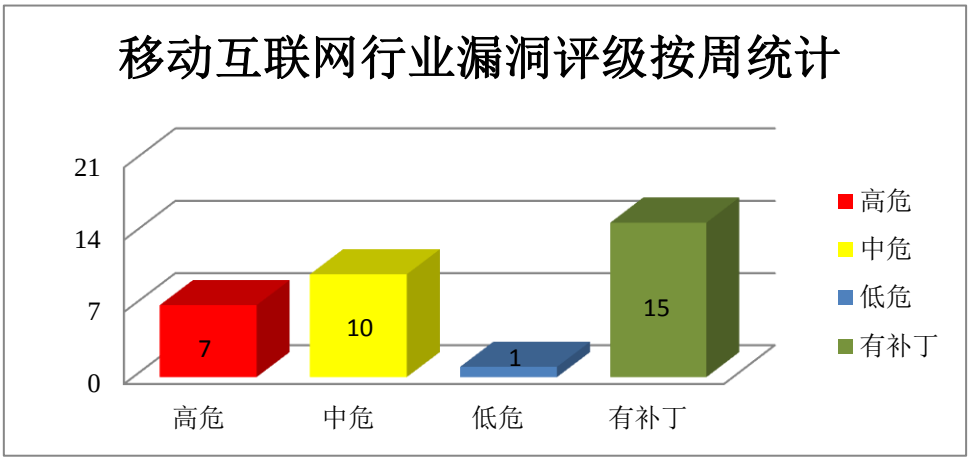

图 4 移动互联网行业漏洞统计

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、CPU 处理器内核存在 Meltdown 和 Spectre 漏洞

CPU hardware 是一套运行在 CPU（中央处理器）中用于管理和控制 CPU 的固件。本周，CPU 处理器内核被披露存在 Meltdown 和 Spectre 漏洞，攻击者可以绕过内存访问的安全隔离机制，使用恶意程序来获取操作系统和其他程序的被保护数据，造成内存敏感信息泄露。

CNVD 收录的相关漏洞包括：CPU 处理器内核存在 Spectre 漏洞、CPU 处理器内核存在 Meltdown 漏洞、CPU 处理器内核存在 Meltdown 漏洞（CNVD-2018-00304）。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-2018-00303

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00302

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00304

2、Western Digital 产品安全漏洞

Western Digital MyCloud NAS 是一款网络连接存储设备。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、上传任意文件或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Western Digital My Cloud NAS 设备拒绝服务漏洞、Western Digital My Cloud NAS 设备跨站请求伪造漏洞、Western Digital My Cloud NAS 设备命令注入漏洞、Western Digital My Cloud NAS 设备无限制文件上传漏洞、Western Digital My Cloud NAS 设备信息泄露漏洞、Western Digital My Cloud NAS 设备硬编码后门漏洞。上述漏洞的综合评级为“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-2018-00400

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00402

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00401

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00403

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00399

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00404

3、Microsoft 产品安全漏洞

Microsoft Windows 10 是一套供个人电脑使用的操作系统，Windows Server 2016 是一套服务器操作系统。Edge 是其中的一个系统附带的默认浏览器。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Edge 和 Microsoft ChakraCore 远

程代码执行漏洞、Microsoft Windows Edge 和 Microsoft ChakraCore 远程代码执行漏洞（CNVD-2018-00324、CNVD-2018-00325、CNVD-2018-00326、CNVD-2018-00327、CNVD-2018-00328、CNVD-2018-00330、CNVD-2018-00331）。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-2018-00329
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00324
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00325
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00326
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00327
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00328
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00330
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00331

4、Apple 产品安全漏洞

Apple macOS High Sierra 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统，tvOS 是一套智能电视操作系统。watchOS 是一套智能手表操作系统，iOS 是一套为移动设备所开发的操作系统，本周，上述产品被披露存在内存破坏、越界读取或输入验证漏洞，攻击者可利用漏洞执行任意代等。

CNVD 收录的相关漏洞包括：Apple iOS 和 macOS High Sierra IOKit 组件内存破坏漏洞、Apple macOS High Sierra Intel Graphics Driver 内存破坏漏洞、Apple macOS High Sierra Intel Graphics Driver 越界读取漏洞、Apple macOS High Sierra IOKit 组件输入验证漏洞、Apple macOS High Sierra IOKit 组件输入验证漏洞（CNVD-2018-00184）、多款 Apple 产品 Kernel 内存破坏漏洞（CNVD-2018-00180、CNVD-2018-00182、CNVD-2018-00183）。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-2018-00185
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00333
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00332
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00186
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00184
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00180
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00182
http://www.cnvd.org.cn/flaw/show/CNVD-2018-00183

5、K7 AntiVirus 空指针解引用漏洞

K7 Antivirus 是印度 K7 Computing 公司的一套反病毒软件。本周，K7 Computing

被披露存在空指针解引用漏洞，攻击者可通过发送 0x95002570 DeviceIoControl 请求利用该漏洞造成拒绝服务（空指针逆向引用）。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 -2018-00250

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-2018-00102	ImageMagick 拒绝服务漏洞（CNVD-2018-00102）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.imagemagick.org/download/beta/
CNVD-2018-00128	DSmall 多用户商城系统存在 SQL 注入漏洞	高	厂商已提供修复方案，请关注厂商主页更新：http://www.csdeshang.com
CNVD-2018-00175	D-Link DSL-6850U 路由器远程命令执行漏洞	高	用户可联系供应商获得补丁信息：http://us.dlink.com/
CNVD-2018-00203	OpenAFS 拒绝服务漏洞（CNVD-2018-00203）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.openafs.org/pages/security/OPENAFS-SA-2017-001.txt
CNVD-2018-00233	Linux kernel 内存错误引用漏洞（CNVD-2018-00233）	高	厂商已发布漏洞修复程序，请及时关注更新：http://lists.openwall.net/netdev/2017/12/04/224
CNVD-2018-00239	Inedo Otter 目录遍历漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://inedo.com/blog/otter-174-released
CNVD-2018-00245	Haystack Arq for Mac helper app 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.arqbackup.com/
CNVD-2018-00257	Umeng Push SDK 导出 Service 组件代码执行漏洞	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.umeng.com/
CNVD-2018-00310	Fossil 任意命令执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.fossil-scm.org/xfer/doc/trunk/www/changes.wiki#v2_4
CNVD-2018-00315	Adobe DNG Converter 存在未明内存破坏漏洞	高	用户可联系供应商获得补丁信息：https://helpx.adobe.com/security/produc

			ts/dng-converter/apsb17-37.html

小结：本周，Western Digital 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、上传任意文件或发起拒绝服务攻击等。此外，Microsoft、Apple、ImageMagick 等多款产品被披露存在多个漏洞，攻击者可利用漏洞上传任意文件、执行任意代码或发起拒绝服务攻击等。另外，K7 Computing 被披露存在空指针解引用漏洞，攻击者可通过发送 0x95002570 DeviceIoControl 请求利用该漏洞造成拒绝服务（空指针逆向引用）。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、Claymore Dual GPU miner 缓冲区溢出漏洞

验证描述

Claymore Dual GPU miner 是一款用于挖矿（虚拟货币计算）的 GPU 监控软件。

Claymore Dual GPU miner 10.1 版本中的远程管理界面的 request handler 存在缓冲区溢出漏洞。远程攻击者可通过较长的 API 请求利用该漏洞执行任意代码。

验证信息

POC 链接：http://www.exploitalert.com/view-details.html?id=28087

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD_-2018-00236

信息提供者

恒安嘉新(北京)科技股份公司

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. Meltdown 与 Spectre：近期 CPU 特性漏洞

2018 年 1 月 4 日，Jann Horn 等安全研究者披露了"Meltdown"(CVE-2017-5754)和"Spectre"(CVE-2017-5753 & CVE-2017-5715)两组 CPU 特性漏洞。据悉，漏洞会造成 CPU 运作机制上的信息泄露，低权级的攻击者可以通过漏洞来远程泄露(浏览器形式)用户信息或本地泄露更高权级的内存信息。目前相关的平台，厂商，软件提供商都在积极应对该系列漏洞，部分厂商提供了解决方案。

参考链接：https://mp.weixin.qq.com/s?__biz=MzU5MjEzOTM3NA==&mid=2247484710&idx=1&sn=9f69312f8c23f4b1be53034d83c362c8&chksm=fe250027c95289313c8c7b4a3811de4e6d5ae8e453c3d1c5df2fc3155c8571ef17cc16e27eb1&mpshare=1&scene=1&srcid=0104

CCzOqnSuWPi210VylZ7l##

2. PHP My Admin 被曝存在严重 CSRF 漏洞

近期，印度安全工程师 Ashutosh Barot 发现 phpMyAdmin 存在严重 CSRF 漏洞（跨站请求伪造），可以通过技巧欺骗管理员去点击构造链接，触发对基于 phpMyAdmin 的 MySQL 数据库的远程操作，实现对数据库的破坏攻击行为。该漏洞对 phpMyAdmin 4.7.x 系列中 4.7.7 之前的所有版本造成影响，目前，phpMyAdmin 官方已发布漏洞修补声明，声明中提到“该漏洞利用方式为，通过欺骗当前登录用户点击某个恶意构造链接，之后可能导致对 MySQL 数据库的记录数据等信息的删除”。

参考链接：http://www.freebuf.com/news/159117.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