迪普科技 2018 年 1 月

信息安全研究月报

杭州迪普科技股份有限公司

Hangzhou DPTech Technologies Co.，Ltd.

目 录

一、 安全漏洞态势

2018 年 1 月份新增安全漏洞 796 个。比上月增加了 126 个，与前 5 个月平均数量相比，安全漏洞数量小幅减少。本月新增的漏洞中，高危漏洞 237 个，中危漏洞 438 个，低危漏洞 121 个，同比 2017 年 1 月（漏洞总数 917 个）减少 13.20%。表 1-1 为 2017 年 8 月-2018 年 1 月漏洞危险等级统计。

表 1-1 2017 年 8 月-2018 年 1 月漏洞危险等级统计

	八月	九月	十月	十一月	十二月	一月
高危	487	524	280	282	392	237
中危	669	569	433	287	247	438
低危	86	107	82	89	31	121
总数	1242	1200	795	658	670	796

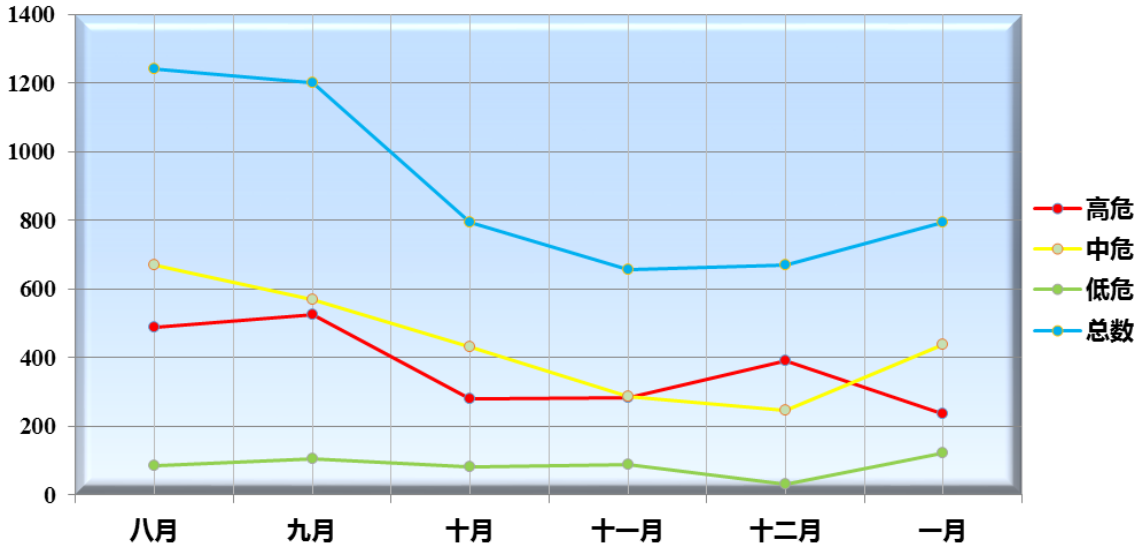

图 1-1 2017 年 8 月-2018 年 1 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 1 月份新增的漏洞类型分布如表 1-2 所示。其中跨站脚本，占 15.83%。值得关注的还有信息泄露、缓冲区溢出和权限许可和访问控制等常见漏洞类型。

表 1-2 2018 年 1 月漏洞类型分布

类型	数量	比例
缓冲区溢出	60	7.54%
权限许可和访问控制	43	5.40%
信息泄露	87	10.93%
输入验证	38	4.77%
跨站脚本	126	15.83%
资源管理错误	12	1.51%
未知	350	43.97%
跨站请求伪造	15	1.88%
SQL 注入	19	2.39%
路径遍历	18	2.26%
其他	28	3.52%

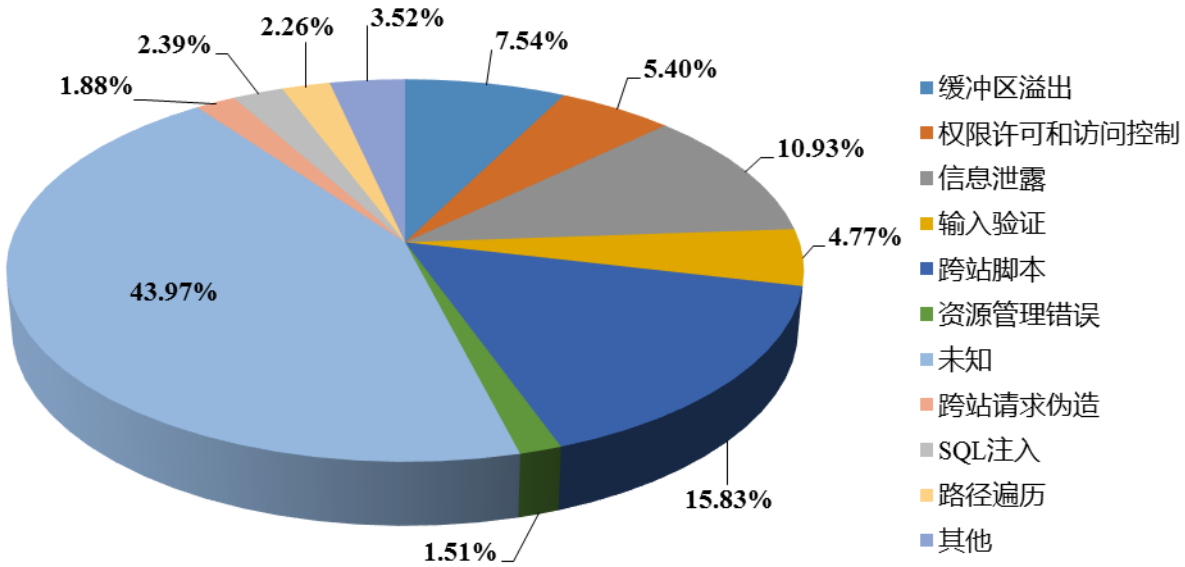

图 1-2 2018 年 1 月漏洞类型占比

三、 高危漏洞实例

(一)主流处理器的多个 CPU 安全漏洞

CVE 编号：CVE-2017-5753、CVE-2017-5715、CVE-2017-5754

CNNVD 编号：CNNVD-201801-150、CNNVD-201801-152、CNNVD-201801-151

发布时间：2018-1

危险等级：☆☆☆☆☆

漏洞类型：信息泄露

受影响软件：

Apple

Google

Intel

Linux Kernel

Microsoft

Mozilla

AMD

ARM

漏洞描述：Intel 处理器爆出多个芯片级高危漏洞，包括 2 个熔断漏洞(Meltdown)和 1 个幽灵漏洞(Spectre)。随着研究深入，发现 AMD 和 ARM 处理器都存在漏洞，使用到这些处理器的上层操作系统(Windows，Linux，macOS，Android 等)也受到影响。

熔断漏洞利用处理器的乱序执行特性进行数据读取。乱序执行完成后处理器会检查当前的乱序是否合理，如果合理处理器将执行后续指令，如果乱序不合理将会回滚到执行前的处理器状态，重新按顺序执行指令。漏洞在于乱序执行已经将内存数据加载到处理器的缓存，而回滚的时候不会同时回滚处理器的缓存数据，攻击者利用侧信道攻击等方式读取缓存，从而可以间接读取到受害进程的任意数据。

幽灵漏洞使用处理器的预测执行特性进行数据读取。预测执行是指处理器为了提升性能，会预测分支并提前执行相关指令。如果实际流程和预测的分支相符，分支指令就得到了提前

执行，如果与预测不相符，处理器会回滚到分支执行之前的状态，读取数据也是通过缓存数据不回滚的特性进行攻击。

利用这些漏洞，攻击者可以绕过内存的安全隔离机制，读取到操作系统上其他进程的敏感数据，进行数据泄露攻击。

修补建议：可以从操作系统补丁方式临时修补（会降低系统运行性能），也可以更换不存在设计缺陷的处理器进行完全修复。及时跟进相关厂商的修复进展：

https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

https://developer.arm.com/support/security-update

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

http://appleinsider.com/articles/18/01/03/apple-has-already-partially-implemented-fix-in-macos-for-kpti-intel-cpu-security-flaw

https://support.apple.com/en-us/HT208394

https://source.android.com/security/bulletin/2018-01-01

https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/

https://my.vmware.com/group/vmware/patch

https://xenbits.xen.org/xsa/advisory-254.html

https://support.google.com/faqs/answer/7622138#chrome

(二)PHP GD 库拒绝服务漏洞

CVE 编号：CVE-2018-5711

CNNVD 编号：CNNVD-201801-587

发布时间：2018-1

危险等级：☆☆☆☆

漏洞类型：拒绝服务

受影响软件：

PHP 5 < 5.6.33

PHP 7.0 < 7.0.27

PHP 7.1 < 7.1.13

PHP 7.2 < 7.2.1

漏洞描述：PHP 是一种被广泛使用的脚本语言，用于基于 Web 的 CGI 程序，它可被安装在包括 Apache、IIS、Caudium、Netscape、iPlanet 和 OmniHTTPd 等多种 Web 服务器上。

该漏洞与 ext/gd/libgd/gd_gif_in.c 文件有关，攻击者利用该漏洞通过精心构造的 GIF 文件，调用 PHP 函数 imagecreatefromgif 或 imagecreatefromstring，触发程序无限循环，耗尽服务器资源，导致拒绝服务，影响网站安全。

远程攻击者可以利用该漏洞对服务器进行拒绝服务攻击，严重危害网站系统安全。

修补建议：尽快升级到最新稳定版本，目前厂商已经发布了升级补丁，补丁获取链接：

http://php.net/ChangeLog-7.php

(三)Electron 远程代码执行漏洞

CVE 编号：CVE-2018-1000006

CNNVD 编号：CNNVD-201801-898

发布时间：2018-1

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Electron ＜ 1.8.2-beta.4

Electron ＜ 1.7.11

Electron ＜ 1.6.16

漏洞描述：Electron 是一个支持使用 JavaScript、HTML 和 CSS 的应用程序开发框架，旨在帮助开发 Atom 编辑器。

该漏洞是由于应用程序在 Windows 上运行时，将自身注册为协议的默认处理程序（例如 myapp://）。如果用户点击了攻击者特制的 url，就会导致远程任意代码执行。无论协议是如何注册的，Windows 注册表或者应用程序的 app.setAsDefaultProtocolClient 的 API，这些应用程序都可能受到影响。该漏洞仅影响 Windows 应用。

攻击者可以利用此漏洞对远程主机进行任意代码执行，严重危害系统安全。

修补建议：尽快升级到最新稳定版本，目前厂商已经发布了升级补丁，补丁获取链接：

https://github.com/electron/electron/releases/tag/v1.8.2-beta.4

https://github.com/electron/electron/releases/tag/v1.7.11

https://github.com/electron/electron/releases/tag/v1.6.16

(四)Oracle Java SE 远程安全漏洞

CVE 编号：CVE-2018-2582

CNNVD 编号：CNNVD-201801-772

发布时间：2018-1

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

Java SE 8u152

Java SE 9.0.1

Java SE Embedded 8u151

漏洞描述：Oracle Java SE 是美国甲骨文（Oracle）公司的产品。Oracle Java SE 用于在桌面和服务器以及目前要求较高的嵌入式环境中开发和部署 Java 应用。

该漏洞与子组件 Hotspot 有关，攻击者可以利用该漏洞通过多种协议访问网络，导致攻击者能对敏感数据进行未经授权的创建、删除或修改。。

该漏洞会导致敏感数据泄露，危害系统安全。

修补建议：尽快更新到最新稳定版本，目前厂商已经发布了升级补丁，补丁获取链接：

http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html

(五)ISC BIND 拒绝服务漏洞

CVE 编号：CVE-2017-3145

CNNVD 编号：CNNVD-201801-833

发布时间：2018-1

危险等级：☆☆

漏洞类型：拒绝服务

受影响软件：

BIND 9.0.0 - 9.8.x

BIND 9.9.0 - 9.9.11

BIND 9.10.0 - 9.10.6

BIND 9.11.0 - 9.11.2

BIND 9.9.3-S1 - 9.9.11-S1

BIND 9.10.5-S1 - 9.10.6-S1

BIND 9.12.0a1 - 9.12.0rc1

漏洞描述：BIND 是互联网上常用的 DNS 服务器软件。

该漏洞与守护进程库 netaddr.c 模块有关，在 BIND 内部处理上游递归获取上下文的清理操作的方式中，进行了不正确的排序，导致了 use-after-free 错误的发生，从而触发断言失败，导致程序崩溃。

远程攻击者可以利用该漏洞对系统进行拒绝服务攻击，危害系统安全。

修补建议：尽快打上该漏洞官方补丁或者升级到最新稳定版本。目前厂商已经发布了升级补丁，补丁获取链接：

http://www.isc.org/downloads

四、 本月安全要闻

(一)黑客攻击 BeeToken 邮件列表，偷走价值 100 万美元以太坊

加密货币初创企业 BeeToken 已被黑客入侵，针对 ICO 并且采用钓鱼攻击，成功盗走价值 100 多万美元的 Ethereum。该公司已在其官方 Twitter 账户上确认这次钓鱼攻击，并警告用户谨慎使用电子邮件和 Telegram 软件，并且表示鼓励用户发送资金可能是欺诈行为。

该公司表示："我们将永远不会通过电子邮件或直接通过 Telegram 软件发送以太坊地址。目前，似乎有几个不同版本的欺诈性电子邮件在网上流传。一些电子邮件也在推动与微软之间不存在的合作关系。

这些钓鱼电子邮件中还包含了一个欺骗性的以太坊地址和一个专门的 QR 码。对于新手投资者来说，特别令人困惑的是，攻击者随着 BeeToken ICO 的正式发布，协调他们的钓鱼电子邮件。事实上，似乎攻击者能够筹集到几乎一半的资金。BeeToken 网站上的一个柜台显示，该网站至今已筹集 230 多万美元。相比之下，与网络钓鱼攻击有关的众多欺诈地址中的三个集体吸引了近 100 万美元。

友情链接：http://hackernews.cc/archives/20515

(二)挪威医疗卫生机构计算机系统遭到入侵，超过 290 万居民信息或将泄露

据外媒报道,位于挪威东南部地区的医疗卫生机构 Health South-East RHF 于 1 月 8 日表示其计算机系统遭到不明人士入侵，可能会影响到约 290 万人（占挪威人口的 56%）的医疗数据。目前相关专家认为该起入侵事件或属境外国家发起的网络间谍活动的涉猎范畴，并表示已采取紧急措施来消除威胁。

根据挪威卫生安全部门 HelseCERT 透露，他们检测到来自 Health South-East RHF 的异常流量，从而发现了入侵行为。研究人员认为在地下网络犯罪中，医疗数据是一种有价值的商品，恶意人士可以将这些数据用于进一步的攻击。专家和政府代表认为，Health South-East RHF 遭受的数据泄露可能是由于境外国家发起的网络间谍活动造成的，因为这些发起者对收集与政府、军方、情报人员和政客有关的数据极为感兴趣。

据悉，Health South-East RHF 为全国约 290 万人提供医疗服务，超出挪威全体居民数目的一半。因此，若医疗数据遭到泄露对于挪威居民将会造成巨大影响。目前 Health South-East RHF 方面表示已采取一系列措施来降低数据泄露可能性及消除威胁。

友情链接：http://hackernews.cc/archives/20047

(三)Strava 健身追踪热度图可能还披露了世界各地的军事基地位置

据外媒报道，Strava 是一家健身追踪软件开发商，其产品能够利用手机 GPS 追踪某位正在健身的用户的时间以及位置，旨在为锻炼者打造一套社交网络。去年 11 月，这家公司发布了一份展示来自世界各地用户体育锻炼的热度图。

而就在近日，来自联合冲突研究所（Institute for United Conflict）的分析师 Nathan Ruser 发现了人们可能根本不会想到的东西——这张地图可以让一些人非常容易地找到军事基地的位置以及那里人员的日常活动。

对此，他在 Twitter 上发布了几张截图来证实他的理论，可以看到，图中可以看到发生在阿富汗的定期慢跑路线、巡逻以及前线作战基地的位置。

实际上，Strava 并不是唯一一个能够显示世界军事设施的地图平台，像谷歌地图以及公共卫星图也都已经能做到这点。但是，谷歌地图显示的是建筑物和道路的位置，而 Strava 则还提供了一些外的信息：它让人们看到目标区域内的运动方式以及频度。

Ruser 指出，任何查看 Strava 热度图的用户都能找到叙利亚的联盟基地、阿富汗的军事设施以及一些未被曝光的美国军事基地。对此，美国中央司令部发言人、空军上校 John Thomas 告诉媒体，军方正在对这幅地图背后进行调查。Strava 发言人则表示，公司一直在努力让用户更好地明白他们的隐私设置，其地图代表的是用户上传至平台的匿名活动数据，但当中并不包括来自被标记为私有或用户定义的隐私区域的活动。

友情链接：http://hot.cnbeta.com/articles/funny/693761.htm?spm=a313e.7916648.0.0.5d2fab1f2GG50M

(四)荷兰三大银行频繁遭受 DDoS 攻击，致其互联网银行服务瘫痪

据外媒报道，荷兰三大银行（荷兰银行、荷兰合作银行以及 ING 银行）于 1 月 29 日表示其网络系统在过去一周内不断遭受分布式拒绝服务（DDoS）攻击，导致网站和互联网银行服务瘫痪。

荷兰银行在上周共遭受 7 次袭击（周末就发生了 3 次），其中包含安全人员在周日晚上观察到的分布式拒绝服务（DDoS）攻击。

荷兰合作银行发言人 Margo van Wijgerden 周一称因网络系统受到 DDoS 攻击，导致网络服务业务下滑。

ING 银行表示，在 DDoS 攻击期间，因为数据流量导致服务器超载，网上银行的可用性承受了巨大压力。

此外，荷兰税务局也遭受了类似攻击，不过其网络服务很快就恢复了运作。

根据相关媒体报道，目前三家银行的一些网络服务已恢复正常运营，并且其官方承诺客户的银行业务细节不会受到损害。

友情链接：http://www.safedog.cn/news.html?id=2513

(五)“百度外卖”平台被非法侵入，4900 万元额度被篡改

“百度外卖”平台系统被非法侵入，4900 余万元额度被篡改，直接消费损失 30 余万元。北京青年报记者 1 月 29 日上午获悉，北京市海淀区人民检察院以涉嫌盗窃罪对犯罪嫌疑人郑某批准逮捕。同时，北京市海淀检察院向新闻媒体通报，该院近日办理了一批犯罪案件，嫌疑人都是利用系统漏洞，为自己刷出天价账户余额，进而消费使用。海淀检方呼吁广大互联网企业要注意防范网络安全漏洞。

据海淀区检察院杨程检察官介绍，2017 年 10 月，北京小度科技有限公司报案，称其旗下的“百度外卖”平台被他人以非法手段篡改系统，将提现金额改为负数，从而实现反向充值自己账户余额，并使用账户余额在“百度外卖”平台上进行消费，总共被篡改 4900 余万元，下单单数覆盖全国多个地区，人数达百余人，直接消费损失 30 余万元。

据解，海淀检察院科技犯罪检察部办理了一批案件，犯罪嫌疑人利用系统漏洞，为自己刷出天价账户余额，进而消费使用。他们中有的人直接通过上述操作给自己的百度外卖账号充值，有的人由他人帮助自己账户进行充值，进而使用账户余额进行消费。2018 年 1 月 4 日，北京市海淀区人民检察院以涉嫌盗窃罪对犯罪嫌疑人郑某批准逮捕。

杨程检察官说，网络上的虚拟数字虚无缥缈，生产出来、消费出去不痛不痒，一些网络硕鼠们利用自己的计算机技术在“互联网+”的浪潮中不去创造财富，反而破坏其他公司的计算机系统满足自己的私欲，其实就是心存侥幸，不惜以身试法。

海淀检方呼吁广大互联网企业要注意防范网络安全漏洞，不给网络硕鼠们以可趁之际，避免一个小小漏洞酿成巨大的经济损失。网民朋友们要恪守法律底线，做合法网民，不要试图利用计算机技术触碰红线，贪小便宜吃大亏，最终落得牢狱之灾。

友情链接：http://www.freebuf.com/news/161583.html

