迪普科技 2018 年 2 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 2 月份新增安全漏洞 981 个。比上月增加了 185 个，与前 5 个月平均数量相比，安全漏洞数量小幅增加。本月新增的漏洞中，高危漏洞 367 个，中危漏洞 502 个，低危漏洞 112 个，同比 2017 年 2 月（漏洞总数 243 个）增长 74.77%。表 1-1 为 2017 年 9 月-2018 年 2 月漏洞危险等级统计。

表 1-1 2017 年 9 月-2018 年 2 月漏洞危险等级统计

	九月	十月	十一月	十二月	一月	二月
高危	524	280	282	392	237	367
中危	569	433	287	247	438	502
低危	107	82	89	31	121	112
总数	1200	795	658	670	796	981

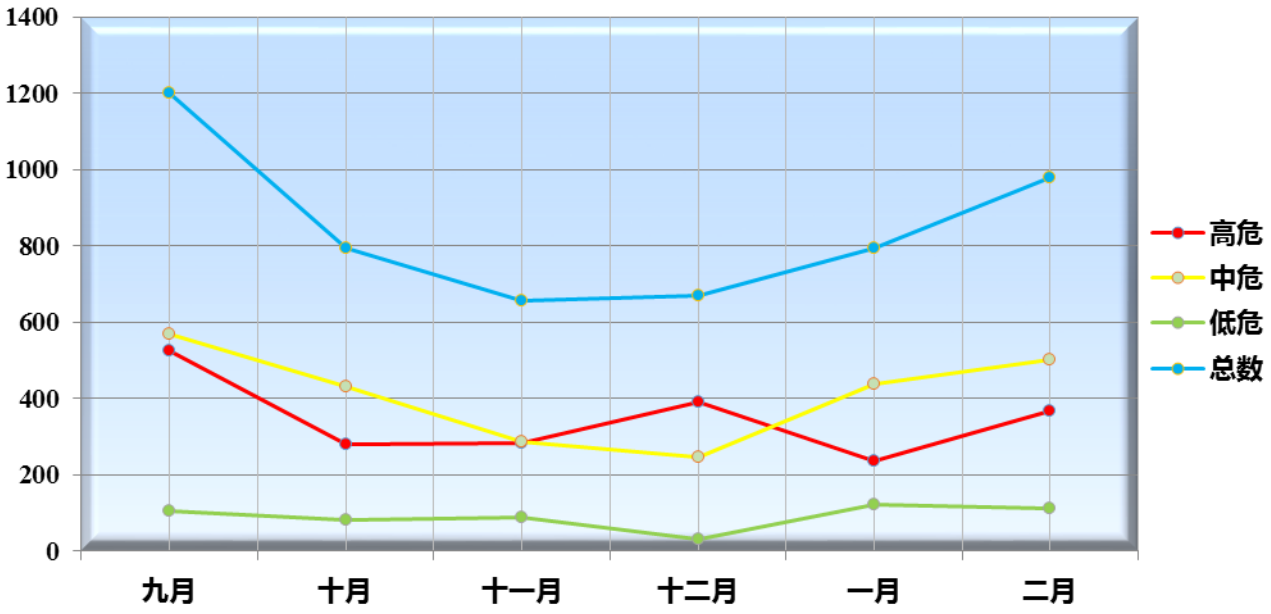

图 1-1 2017 年 9 月-2018 年 2 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 2 月份新增的漏洞类型分布如表 1-2 所示。其中信息泄露，占 13.22%。值得关注的还有缓冲区溢出、跨站脚本和权限许可和访问控制等常见漏洞类型。

表 1-2 2018 年 2 月漏洞类型分布

类型	数量	比例
未知	339	34.56%
缓冲区溢出	120	12.23%
信息泄露	120	12.23%
跨站脚本	106	10.81%
权限许可和访问控制	77	7.85%
输入验证	64	6.52%
数字错误	28	2.85%
SQL 注入	26	2.65%
资源管理错误	20	2.04%
跨站请求伪造	18	1.83%
其他	63	6.42%

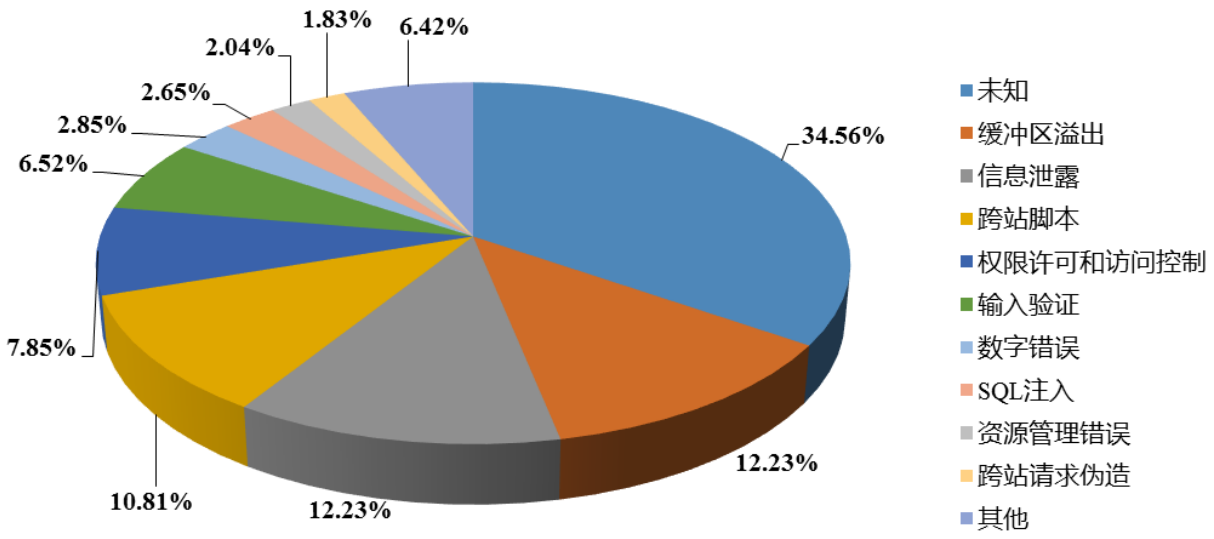

图 1-2 2018 年 2 月漏洞类型占比

三、 高危漏洞实例

(一)Adobe Flash 0day 漏洞

CVE 编号：CVE-2018-4878

CNNVD 编号：CNNVD-201802-043

发布时间：2018-02

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Adobe Flash Player <= 28.0.0.137

漏洞描述：Adobe Flash Player 是美国奥多比（Adobe）公司的一款兼容性高、基于浏览器的多媒体程序播放器产品，能够在多种浏览器、操作系统和移动设备上使用，超过 13 亿台连接 Internet 的桌面计算机和移动设备上都安装了 Adobe Flash Player。

该漏洞存在于 Adobe Flash Player 28.0.0.137 及其之前的所有版本中。该漏洞是由于 Flash 的 com.adobe.tvsdk 包中的 DRMManager 对象，相关的调用没有正确处理导致释放后重用（Use-After-Free）漏洞，通过修改 ByteArray 对象的 Length 可以实现任意内存读写执行，执行最终的 shellcode 代码。

攻击者可以利用该漏洞远程执行任意代码，进一步获取服务器权限，危害服务器安全。

修补建议：目前厂商已经发布了升级补丁以修复此漏洞，补丁获取链接：

https://helpx.adobe.com/security/products/flash-player/apsb18-03.html

(二)WordPress 通杀 DoS 漏洞

CVE 编号：CVE-2018-6389

CNNVD 编号：CNNVD-201802-159

发布时间：2018-02

危险等级：☆☆☆☆☆

漏洞类型：设计缺陷

受影响软件：

Wordpress Wordpress <= 4.9.2

漏洞描述：WordPress 是一种使用 PHP 语言开发的开源的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站，并逐步演变成一款小型的 CMS，很多非博客网站也是用 WordPress 搭建的。

该漏洞是一个应用程序级别的 DoS 攻击漏洞，该漏洞存在于 load-scripts.php 文件中，load-scripts.php 文件是为 WordPress 管理员设计的内置脚本，用于处理用户定义的请求。为保证管理员登录前就在管理登录页面，load-scripts.php 中没有做任何的认证，这就导致该页面可以被任意访问。通过少量请求返回大数据，造成服务器资源消耗，从而导致 DoS 攻击。

攻击者可利用此漏洞用很小的带宽来达到网络级 DDoS 攻击的效果 达到拿下 WordPress 站点的目的。

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://wordpress.org/

(三)Apache Tomcat 安全机制绕过漏洞

CVE 编号：CVE-2018-1305、CVE-2018-1304

CNNVD 编号：CNNVD-201802-564、CNNVD-201802-668

发布时间：2018-02

危险等级：☆☆☆☆

漏洞类型：信息泄露

受影响软件：

Apache Tomcat 9.0.0.M1 - 9.0.4

Apache Tomcat 8.5.0 - 8.5.27

Apache Tomcat 8.0.0.RC1 - 8.0.49

Apache Tomcat 7.0.0 - 7.0.84

漏洞描述：Apache Tomcat 是美国 Apache 软件基金会的 Jakarta 项目的一款轻量级免费的开放源代码的 Web 应用服务器，主要用于开发和调试 JSP 程序。

由于 Apache Tomcat 的 servlet 注释定义的安全约束，只在 servlet 加载后才应用一次，适用于 URL 模式及该点下任何 URL。由于 Servlet 加载的顺序，某些安全约束会失去作用，这可能会将资源暴露给未被授权访问的用户。

攻击者可以利用该漏洞获取被限制的信息，导致敏感信息泄露。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：https://lists.apache.org/thread.html/d3354bb0a4eda4acc0a66f3eb24a213fdb75d12c7d16060b23e65781@%3Cannounce.tomcat.apache.org%3E

(四) Joomla!跨站脚本漏洞

CVE 编号：CVE-2018-6379

CNNVD 编号：CNNVD-201801-1084

发布时间：2018-02

危险等级：☆☆☆

漏洞类型：远程代码执行

受影响软件：

Joomla! 1.5.0 - 3.8.3

漏洞描述：Joomla!是美国 Open Source Matters 团队开发的一款开源的内容管理系统（CMS）,该系统可以实现批量管理、网站搜索等功能,可以运行在 Linux、Windows、MacOSX 等各种不同的平台上。

该漏洞是由于未对用户的输入进行正确的过滤。攻击者可以利用该漏洞在受影响的浏览器中执行任意脚本代码，可能导致基于 cookie 的身份验证凭据被窃取。

攻击者可以利用此漏洞远程执行代码，获取 cookie 信息，进一步实施攻击行为，危害服务器安全。

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://developer.joomla.org/security-centre/721-20180104-core-xss-vulnerability.html

(五) ISC BIND9 远程 DoS 漏洞

CVE 编号：CVE-2017-5734

CNNVD 编号：None

发布时间：2018-02

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

ISC Bind 9.10.6-S2

ISC Bind 9.10.6-S1

ISC Bind 9.10.5-S4

ISC Bind 9.10.5-S3

ISC Bind 9.10.5-S2

ISC Bind 9.10.5-S1

漏洞描述：ISC BIND 是美国 Internet Systems Consortium（ISC）公司的一款实现了 DNS 协议的开源软件，是目前全球最为通用的域名解析软件。

该漏洞与 badcache.c 模块有关，在处理特定类型的畸形数据包 BIND 时，会错误地选择 SERVFAIL rcode 而不是 FORMERR rcode。如果接收视图启用了 SERVFAIL 缓存功能，当请求不包含所有预期信息时，可能会触发断言失败，导致程序崩溃。

攻击者可以利用该漏洞发起 DOS 攻击，使程序崩溃，服务器宕机。

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5734

四、 本月安全要闻

(一)瑞士电信数据泄露 80 万客户数据，瑞士 10%公民个人信息受威胁

瑞士电信公司 Swisscom 证实，其数据泄露已经影响到大约 80 万名客户，大约占瑞士人口的 10%。这是 2018 年第三起国家级的数据泄露事件。

根据瑞士电信公司的说法，攻击者使用销售伙伴的凭证访问了客户的记录。安全漏洞是瑞士电信在例行检查中发现的，大部分暴露的数据都与移动服务用户有关。该公司发布的新闻稿中写道。“2017 年秋，不明身份者挪用了销售合作伙伴的访问权限，未经授权访问了客户的姓名、地址、电话号码和出生日期。根据数据保护法，这一数据被归类为‘不敏感’。”

泄露的这些数据，电信巨头收集这种类型的数据时，与客户签署了订阅协议。目前尚不清楚黑客是如何获得证书的，好消息是销售合作伙伴只能访问客户身份信息和管理合同。

Swisscom 强调说，根据数据保护法律，入侵者访问的数据视为不敏感数据，但无论如何，这些公民个人信息是地下犯罪分子的珍贵商品，因为骗子可以利用这些数据对他们的客户进行网络钓鱼攻击。

瑞士电信已经向瑞士联邦数据保护和信息专员（FDPIC）报告了数据泄露事件。新闻稿称“该系统没有被黑客入侵，密码、通话或支付数据等敏感数据并未受到事件的影响，”

瑞士电信数据泄露后，该公司撤销了用于访问其系统的凭证，并对合作伙伴实施更严格的控制。

友情链接：http://toutiao.secjia.com/swisscom-databreach

(二)科罗拉多交通部感染 SamSam 勒索软件，被迫关闭 2000 台电脑

据外媒 2 月 23 日报道，科罗拉多州交通部（DOT）于本周三发生了一起勒索事件—黑客利用 SamSam 勒索软件感染 DOT 计算机系统，并以恢复数据为要挟条件来获取比特币赎金。不过日前 DOT 方面已采取了补救措施，但其表示不会通过支付赎金的方式，而是选择关闭 2000 多台员工计算机设备。

SamSam 是一款由单个团体部署的勒索软件，在 2016 年冬季被广泛使用。但据媒体介绍，目前黑客组织似乎准备利用 SamSam 开展新的攻击活动。

研究人员介绍了 SamSam 的部署方式：攻击者通过暴力破解 RDP 连接来访问公司内部网络，从而感染目标设备系统，以达到利用 SamSam 勒索软件加密相关文件的目的。

在最近的一些攻击活动中，SamSam 运营商通常会要求受害用户支付 1 比特币赎金，并在其计算机上留下“我很抱歉”的消息。

此外，研究人员还发现在今年 1 月份感染医院、市议会以及 ICS 公司的勒索软件似乎也是 SamSam。目前根据初步统计结果显示，黑客组织从这些攻击中赚取的赎金已超过 30 万美元。其中印第安纳州的一家受害医院在有备份数据的情况下也同意支付黑客 55,000 美元的赎金需求，因为该医院认为支付赎金比从备份恢复所有计算机数据更容易、更快。

但 DOT 表示，他们不会屈服黑客的赎金威胁，将会选择从备份中恢复数据。交通部官员告诉当地媒体其关键系统受到影响，例如管理道路监控摄像头、交通警报、留言板等重要模块。除此之外，DOT 的 IT 人员也正在与其防病毒提供商 McAfee 合作，在将 PC 重新引入网络之前，对受影响的工作站进行补救，并保护其他终端。

友情链接：http://hackernews.cc/archives/21016

(三)任天堂 Switch 遭 fail0verflow 黑客组织破解，已可运行 Linux 系统

fail0verflow 黑客组织成员近日在赫赫有名的游戏机 NintendoSwitch 上发现了一个漏洞，他们在推特上公开了他们的发现，并发布了漏洞利用的结果——成功在 Switch 上安装并运行 Debian Linux 发行版！

他们表示任天堂 Switch 中存在漏洞，且目前无法通过固件更新进行修复，他们进行漏洞利用后即可安装 Linux 系统。

fail0verflow 组织一直致力于破解各种主机平台。他们目前发现的漏洞，是在 Nividia Tegra X1 系统的 boot ROM 上。在 Switch 游戏设备启动的时候，漏洞利用程序能够触发 ROM 中的漏洞，目前软件和固件更新并不能解决这个漏洞问题，因为只要用户开启电源就会加载这个 ROM。

在 Boot ROM 上发现漏洞，而目前并没有合适的修复方案，可谓打开了 Switch 的新世界大门：可能会引发其他目标的入侵？泄漏隐私数据？

或者在不远的将来，黑客可能可以寻找到安装 homebrew 应用的方法，安装盗版游戏等等。

而对于任天堂方面，在此次破解之后，他们可能需要紧密地与 Nividia 合作，寻找 Tegra X1 芯片上的加固方案，或者给出一种暂时性的解决方案，阻止用户使用破解后的主机。

友情链接：http://www.freebuf.com/news/162756.html

(四)惨遭黑客洗劫，意大利交易所 BitGrail 损失 1.7 亿美元加密货币

本周五，一家名为 BitGrail 的意大利加密货币交易所表示，它损失了约 1700 万个名为 Nano 的加密货币代币，市值大约为 1.7 亿美元。

该交易所在刊登在其网站上的一个通知中表示：“内部的检查发现了未经授权的交易，导致 BitGrail 管理的钱包中产生了 1700 万 Nano 代币的缺口。”不过，它并未透露是何时遭到了黑客攻击。

该交易所已经将这一情况通知了当局，而且它不认为所持有的其他货币也受到了影响。不过，它确实表示将暂时中止所有的提现和存入交易。据悉，BitGrail 的代表直到纽约时间周五晚上仍无法联系。

但是一个名为“Francesco the Bomber”的疑似交易所运营者的 Twitter 用户，在公告发布之后偶，在其社交媒体网站上发表了几条评论。其中一条说道：“我们是有透明度的，但资金被盗了。”另一条推文说道：“警方正在进行调查。”

这位 Twitter 用户也表示，交易所无法赔偿客户的损失。此外，他还提到了针对他的“毫无根据的指控”。

在加密货币领域，最知名的黑客攻击案件是日本交易所 Mt.Gox 于 2014 年遗失价值 4.6 亿美元加密货币的事件。在如 Equifax 或美国人事管理办公室等知名黑客入侵事件中，往往涉及到的是数据，而加密货币对于黑客来说是另一个非常诱人的目标。由于它们不可撤回的属性，比特币和其他加密货币的交易是无法删除的。也就是说，一旦黑客将比特币从目标在线钱包中移动到他们自己的账户中，是很难将其追回的。

友情链接：http://www.lieyunwang.com/archives/412775

(五)巴黎 Octoly 公司因亚马逊 S3 存储错误配置，泄露全球 12000 明星/网红个人信息

外媒 2 月 6 日消息，UpGuard 安全研究人员发现，巴黎 Octoly 公司因其亚马逊 S3 存储桶错误配置，导致超过 12,000 名社交媒体影响者（俗称：明星或网红）的敏感数据在线暴露。据悉，这些用户大多来自 YouTube、Instagram、Twitter 和 Twitch 等社交平台，目前 Octoly 公司担心竞争对手利用该暴露事件乘机抢夺这些平台的用户资源。

Octoly 是一家总部位于巴黎的品牌营销公司，致力于向社交媒体明星提供来自顶级品牌的产品，并寻求其评论以及认可。Octoly 的客户包括迪奥、丝芙兰、欧莱雅、雅诗兰黛、兰蔻以及游戏巨头育碧和暴雪娱乐等。

UpGuard 网络风险团队总监 ChrisVicker 于 1 月初发现，一个配置错误、并且可公开访问的亚马逊网络服务（AWS）S3 云存储桶被 Octoly 公司用来存储内部重要文件。这些文件包括：用户敏感信息（真实姓名、地址、电话号码、电子邮件地址以及出生日期）；使用 bcrypt 加密的 Octoly 账户散列密码；大量的品牌和分析信息（Octoly 服务的 600 个品牌的清单，以及受影响用户的“深度社交”报告）。

Upguard 认为，该暴露事件可能会在一定程度上影响 Octoly 公司的日常运营。并且 Upguard 表示该暴露事件所带来的最大风险不在于经济损失，而在于人，因为泄露的用户资料让竞争对手有了可乘之机，各大品牌可能会争抢知名社交媒体影响者的青睐。

友情链接：http://hackernews.cc/archives/20716

