迪普科技 2017 年 7 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.

版权所有 侵权必究 All rights reserved

目 录

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

一、 安全漏洞态势

2017 年 7 月份新增安全漏洞 1063 个。比上月增加了 238 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 483 个，中危漏洞 506 个，低危漏洞 74 个，同比 2016 年 7 月(漏洞总数 724 个)增长 46.82%。表 1-1 为 2017 年 2 月-2017 年 7 月漏洞危险等级统计。

表 1-1 2017 年 2 月-2017 年 7 月漏洞危险等级统计

	二月	三月	四月	五月	六月	七月
高危	367	402	535	283	319	483
中危	502	602	564	312	398	506
低危	112	107	97	63	108	74
总数	981	1111	1196	658	825	1063

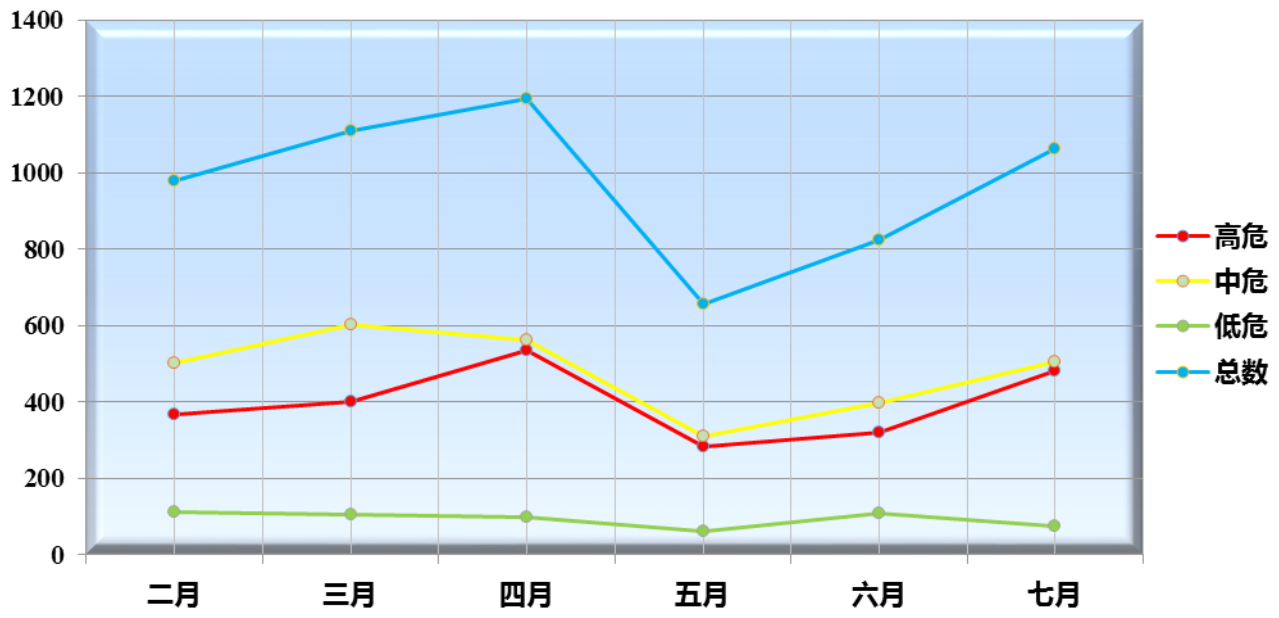

图 1-1 2017 年 2 月-2017 年 7 月漏洞新增数量趋势

二、 漏洞类型分布

2017 年 7 月份新增的漏洞类型分布如表 1-2 所示。其中缓冲区溢出占比例较大，占 16.50%。值得关注的还有信息泄露、输入验证与权限许可和访问控制等常见漏洞类型。

表 1-2 2017 年 7 月漏洞类型分布

类型	数量	比例
缓冲区溢出	233	21.92%
权限许可和访问控制	88	8.28%
信息泄露	56	5.27%
输入验证	50	4.70%
跨站脚本	107	10.07%
资源管理错误	24	2.26%
未知	145	13.64%
授权问题	16	1.51%
路径遍历	11	1.03%
SQL 注入	30	2.82%
其他	303	28.50%

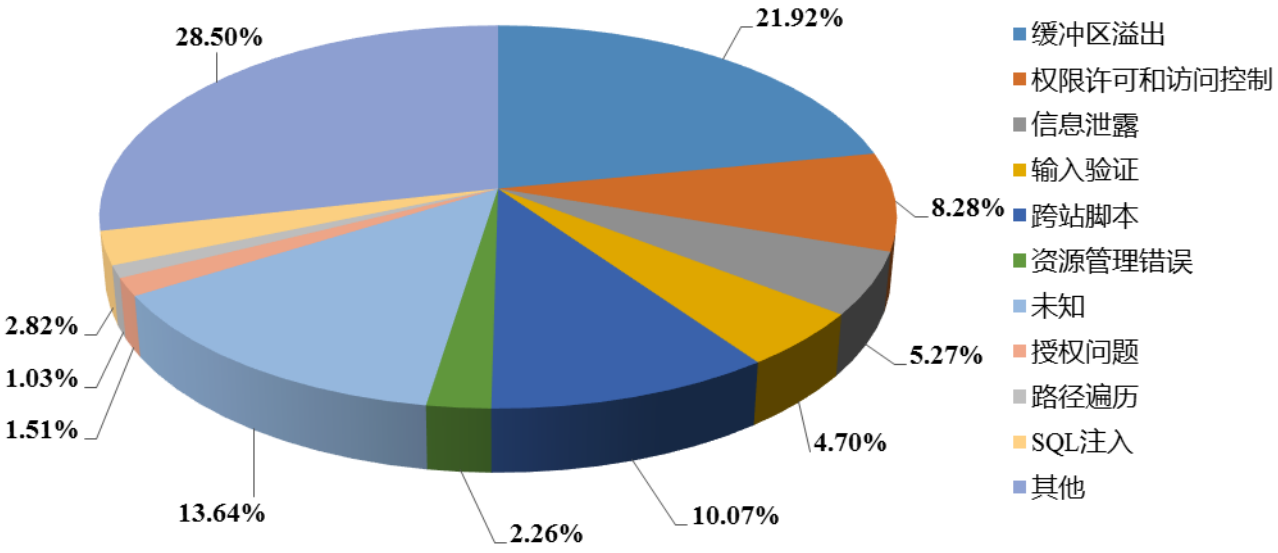

图 1-2 2017 年 7 月漏洞类型占比

三、 高危漏洞实例

(一)Apache Struts2 远程代码执行漏洞(S2-048)

CVE 编号：CVE-2017-9791

CNNVD 编号：CNNVD-201706-928

发布时间：2017-7

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Apache Struts 2.3.X

漏洞描述：Struts 2 是美国 Apache 软件基金维护的一个开源项目，也是采用 Java Web 构建的网站系统常用的一款框架。Struts 2 框架引入了 OGNL 表达式，OGNL 表达式允许开发者使用标签方便地访问 ActionContext 等相关变量。OGNL 表达式存在的问题在于计算这种表达式的时候，有机会执行系统命令。如果黑客提交的参数，能进入 OGNL 表达式的计算流程，就可能造成任意代码执行漏洞。近年来 Struts 2 框架相关的高危漏洞(如 2013 年的 S2-016,2014 年的 S2-019,S2-020，2016 年的 S2-032,S2-037 等)主要原因就是 OGNL 表达式。

近日曝出的 Struts2 高危漏洞(S2-048)，是由于 Struts2-Struts1 插件的 jar 包存在问题，用户提交的参数会通过该 jar 包的 Gangsterform.getName 函数，逐步代入到 OGNL 表达式执行，获得命令执行的机会，从而造成攻击。

该漏洞是框架漏洞，可以进行任意代码执行，影响广泛，危害极大。

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：

https://cwiki.apache.org/confluence/display/WW/S2-048?from=timeline&isappinstalled=0

(二)Nginx 远程信息泄露漏洞

CVE 编号：CVE-2017-7529

CNNVD 编号：CNNVD-201707-563

发布时间：2017-7

危险等级：☆☆☆☆☆

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

漏洞类型：信息泄露

受影响软件：

Nginx 0.5.6 - 1.13.2

漏洞描述：Nginx 是一款轻量级 Web 服务器及电子邮件代理服务器。

该漏洞是由于程序没有对用户提交的数据进行正确的边界检测。在 Nginx 的 range filter 中存在整数溢出漏洞，当使用 Nginx 标准模块时，Nginx 通过缓存返回响应内容，攻击者会获取到缓存文件头，通过带有特殊构造的 range 的 HTTP 头的恶意请求引发该漏洞，可能获取到后端服务器 IP 地址等其他敏感信息，导致信息泄露。

远程攻击者可直接利用该漏洞获取敏感信息，造成数据泄露的影响。

修补建议：禁用 multipart range 功能，在 Nginx 配置文件中添加 max_ranges 1。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://mailman.nginx.org/pipermail/nginx-announce/2017/000200.html

(三)Redhat NTP 任意代码执行漏洞

CVE 编号：CVE-2017-6458

CNNVD 编号：CNNVD-201703-105

发布时间：2017-7

危险等级：☆☆☆☆

漏洞类型：代码执行

受影响软件：

NTP < 4.2.8p10

NTP 4.3.x < 4.3.94

漏洞描述：NTP，网络时间协议，是一款通过网络同步计算机时钟的协议。

该漏洞与‘ctl_put*’函数有关，如果在 ntp.conf 文件中配置了自定义字段，且字段名称很长，当它将用户提供的数据复制到缓冲区的时候，并不能正确的判断缓冲区的大小是否足够，则包含这些字段的响应数据包会导致缓冲区溢出。

攻击者可以利用此漏洞在受影响的应用程序内的上下文中执行任意代码，严重危害主机安全。失败的尝试也会导致拒绝服务。

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

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://support.ntp.org/bin/view/Main/NtpBug3379

(四)Microsoft Skype 缓冲区错误漏洞

CVE 编号：CVE-2017-9948

CNNVD 编号：CNNVD-201706-1098

发布时间：2017-7

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Microsoft Skype 7.37 之前的 7.2 版本

Microsoft Skype 7.37 之前的 7.35 版本

Microsoft Skype 7.37 之前的 7.36 版本

漏洞描述：Skype 是一套即时通讯软件，允许用户通过文字、语音和视频等方式进行即时通信。

该漏洞存在于 Skype Web 消息与语音呼叫服务中，攻击者利用一个低权限的 Skype 用户账号，通过目标计算机系统的剪切板将特制的恶意图像文件复制粘贴到 Skype 程序的会话窗口中，当恶意图像文件同时保存在远程系统和本地系统的剪切板中，Skype 程序便会发生栈缓冲区溢出，执行代码。

攻击者可以利用此漏洞对远程主机进行栈缓冲区溢出攻击，执行代码，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：

https://www.skype.com/de/download-skype/skype-for-windows/downloading/

(五)Apache HTTP Server mod_http2 空指针间接引用漏洞

CVE 编号：CVE-2017-7659

CNNVD 编号：CNNVD-201706-890

发布时间：2017-7

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

危险等级：☆☆☆

漏洞类型：空指针引用

受影响软件：

Apache Group HTTP Server 2.4.25

Apache Group HTTP Server 2.4.24

漏洞描述：Apache HTTP Server 是 Apache 软件基金会的一个开放源代码的网页服务器，是最流行的 Web 服务器端软件之一。

满足以下三个条件会触发该漏洞：HTTP 版本为 1.0；没有 Host 头；服务器支持 HTTP/2。在处理构造的 HTTP/2 请求时，会造成 mod_http2 间接引用空指针（r->hostname 为空），导致服务器进程崩溃。

攻击者可以利用此漏洞造成服务器进程崩溃，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://lists.apache.org/thread.html/1d0b746bbaa3a64890fcdab59ee9050aaa633b7143e7d412374e5a9a@%3Cannounce.httpd.apache.org%3E

四、 本月安全要闻

(一)意大利银行巨头 UniCredit 遭黑客入侵，40 万客户信息在线泄露

24 日夜间至 25 日凌晨，意大利最大银行之一的 UniCredit 银行信息系统发出报警，银行内部系统遭到黑客入侵，近 40 万客户的个人贷款信息被泄露。

意大利《晚邮报》26 日报道，UniCredit 银行的客户银行贷款信息、客户个人信息及银行卡卡号(IBAN)均已被泄露。但用户账户密码及其他用于登录账户的信息、户头存款及支出情况、信用卡类敏感信息并未被泄密，因此，不法分子暂时还无法完成非法转账类活动。

UniCredit 银行透露，首次发生黑客攻击事件是在 2016 年 9 月至 10 月，第二次则发生在今年 6 月及 7 月。目前，UniCredit 银行已将此情况通知了政府有关部门，并组成特别审查小组对事件展开调查。

据报道，米兰市检察院已在 26 日对案件出具了调查报告。同时，因受到这一事件影响，26 日 UniCredit 银行股市已下跌 0.7 个百分点。

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

事发后，银行已立即采取措施以避免事态进一步扩大，并将保护客户信息作为当下“绝对首要”任务。同时，银行表示将在“Transform 2019”战略计划中投资 23 亿欧元，用于加强信息系统的安全。

专门负责管理 UniCredit 集团电脑信息的 Ubis 公司首席执行官 Daniele Tonella 告诉路透社记者：“目前还不清楚黑客发起攻击的动机”，他同时强调，“目前并未有任何银行密码及任何用于转账的信息遭到泄露。”

网络安全公司 CSE Cybsec Enterprise 首席技术长官 Sera Pierluigi Paganini 认为：“IBAN 号是所有诈骗类活动的出发点。犯罪分子可以通过钓鱼网站伪装成银行网站，并向用户发送邮件，再以窃取到的个人信息和 IBAN 号骗取用户信任，要求用户输入其他敏感信息。”

友情链接：http://www.ankki.com/AboutNewsDetail_84_1211.html

(二)美国 Mandiant 网络安全公司疑遭黑客入侵，部分文件可公开下载

美国网络安全公司 Mandiant Corporation 是一家位于美国加州的拥有军方背景的私人网络安全技术公司。创始人凯文·曼迪亚（Kevin Mandia）是美国空军情报中心退役军官。其在 2013 年 2 月 19 日公布了指责中国军方黑客袭击 141 家企业的细节追踪报告，指证称中国军方窃取了这些企业的商业机密。

2013 年 12 月 30 日，网络安全公司 FireEye 以 10 亿美元收购了麦迪安网络安全公司。

据悉，今天下午某黑客组织声称其通过入侵美国网络安全公司 Mandiant Corporation 一位高级威胁情报分析师的个人电脑，渗透进公司内网获取大量机密资料。这些机密资料包括网络拓扑图（可能是 FireEye 的核心分析实验室）、完整的业务和个人电子邮件 dump 等信息。

该黑客组织在公告中表示“此次泄漏只是向你们展示一下我们已经深入到 Mandiant 什么地方了，我们可能会在未来发布更多的关键数据。所以千万别惹我们哦！”

友情链接：http://bobao.360.cn/news/detail/4244.html

(三)Google Groups 配置错误导致数百家企业机密数据在线曝光

Google Groups 作为企业协作工具与交流平台，负责团队通信维护与邮件管理。当这些电子邮件组被设置为公开状态而非内部共享时，无需成为内部成员即可公开查看成员之间发送的内部消息。

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

RedLock 研究人员发现，此次事件致使受害企业员工电子邮件地址与内容，以及员工薪酬补偿、销售渠道数据、客户密码、姓名与家庭地址等个人身份信息在线泄露，可供全球用户任意查看。

值得深思的是，引发这起数据泄露事件并非安全漏洞，仅是 Google Groups 功能设置。但这一事件表明，任何一次操作疏忽都将对企业产生毁灭性影响。一旦网络犯罪分子获取这些企业信息，就可用来劫持企业帐户、开展网络钓鱼攻击以及在线泄露敏感谈话内容等。

目前，为防止数据信息再次泄露，研究人员建议各企业立即检查 Google Groups 设置，确保访问权限设置为“不公开”，以确保域名访问权限切换至内部成员使用。

RedLock 首席执行官兼联合创始人瓦伦·巴德瓦尔（Varun Badhwar）表示：“即使再简单的配置错误都带来极其严重的潜在破坏性，无论是在 SaaS 应用还是云计算基础架构中 。”

Badhwar 指出，诸如 Deep Root Analytics、WWE 和 Booz Allen Hamilton 的数据泄露事件，就是因为这样简单的错误配置引发的。

RedLock CSI 团队发现的这个新问题可能会导致数百家企业的敏感信息遭到泄露，而这只需要点击一个按钮即可。在当今互联网环境，每个企业都应该采取必要的措施，要求员工去了解安全操作规范以及利用自动化进程的安全应用程序和其他系统流程工具。例如，在云计算中，一个资源平均只存在 127 分钟，单靠 IT 团队，无法跟上这种快速的变化。

友情链接：http://wemedia.ifeng.com/23694371/wemedia.shtml

(四)印度发生最大规模数据泄漏事件，超过 1 亿用户信息被曝

近日，有印度媒体发现，Reliance Jio 的一亿多用户的数据被泄漏到 Magicapk.com 网站上，包括姓名、手机号、电子信箱、SIM 激活日期，甚至还包括 Aadhaar 号码（身份识别信息）。

业内人士认为，如果消息属实，这可能是印度电信史上最大规模的用户数据泄漏事件。目前，Reliance Jio 正在调查此事，但已初步表示，Magicapk.com 网站上发布的数据似乎是“不真实的”。

Reliance Jio 还称，它们对用户数据采用了最高等级加密，非常安全。但是，已经有许多 Reliance Jio 用户在 Twitter 上抱怨，称自己的个人资料被曝光。此外，一些印度媒体经过调查后也证实，Magicapk.com 上的数据是真实的。

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved

对此，Reliance Jio 一发言人称：“针对数据泄露一事，我们已经通知了执法部门，将来我们还会继续跟进。”

针对所谓的“用户数据泄露”事件，印度电信运营商 Reliance Jio 日前表示，正在对此展开调查。Reliance Jio 由印度首富穆克什·安姆巴尼（Mukesh Ambani）创建，去年 9 月正式运营。通过提供免费的 4G 服务，Reliance Jio 迅速吸引了 1 亿多用户。

友情链接：https://www.easyaq.com/news/2049368798.shtml

(五)美国电视媒体 HBO 遭黑客入侵，《权力的游戏》等热门剧集被盗

美国有线电视频道 HBO 于本周一（7 月 31 日）称，黑客盗取了该品牌即将推出的节目，包括热门剧集《权力的游戏》（Game of Thrones）尚未播出的一季脚本。目前，隶属于时代华纳旗下 HBO 就具体有哪些节目被盗的问题拒绝置评。

HBO 董事长理查德·普莱普勒（Richard Plepler）确认消息后在发送给员工的一封邮件中写道：“正如大多数人已经听说的那样，公司遭遇黑客袭击，其结果导致某些专有信息被盗，包括尚未播出的热门节目等。目前，执法官员已展开调查。此外，任何侵略性质的行为都是具有破坏性、令所有人都感到不安。不幸的是，摆在大家面前的问题是世界非常熟悉的，现在我们自己也身处其中。”

根据《娱乐周刊》（Entertainment Weekly）报道，黑客盗取了 1.5TB 的数据，并已在网上公布了《球手》和《104 号房间》的未播出剧集。另外，还有定于下周播出的《权力的游戏》最新剧集的“一个脚本或情节梗概”。路透社表示，他们于上周日就已收到一封电子邮件，发件人自称盗取了 HBO 数据，其中包括《权力的游戏》相关数据。

友情链接：http://hackernews.cc/archives/12957

杭州迪普科技股份有限公司 版权所有，侵权必究 All rights reserved