迪普科技 2017 年 9 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

2017 年 9 月份新增安全漏洞 1200 个。比上月减少了 42 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 524 个，中危漏洞 569 个，低危漏洞 107 个，同比 2016 年 9 月(漏洞总数 575 个)增长 108.70%。表 1-1 为 2017 年 4 月-2017 年 9 月漏洞危险等级统计。

表 1-1 2017 年 4 月-2017 年 9 月漏洞危险等级统计

	四月	五月	六月	七月	八月	九月
高危	535	283	319	483	487	524
中危	564	312	398	506	669	569
低危	97	63	108	74	86	107
总数	1196	658	825	1063	1242	1200

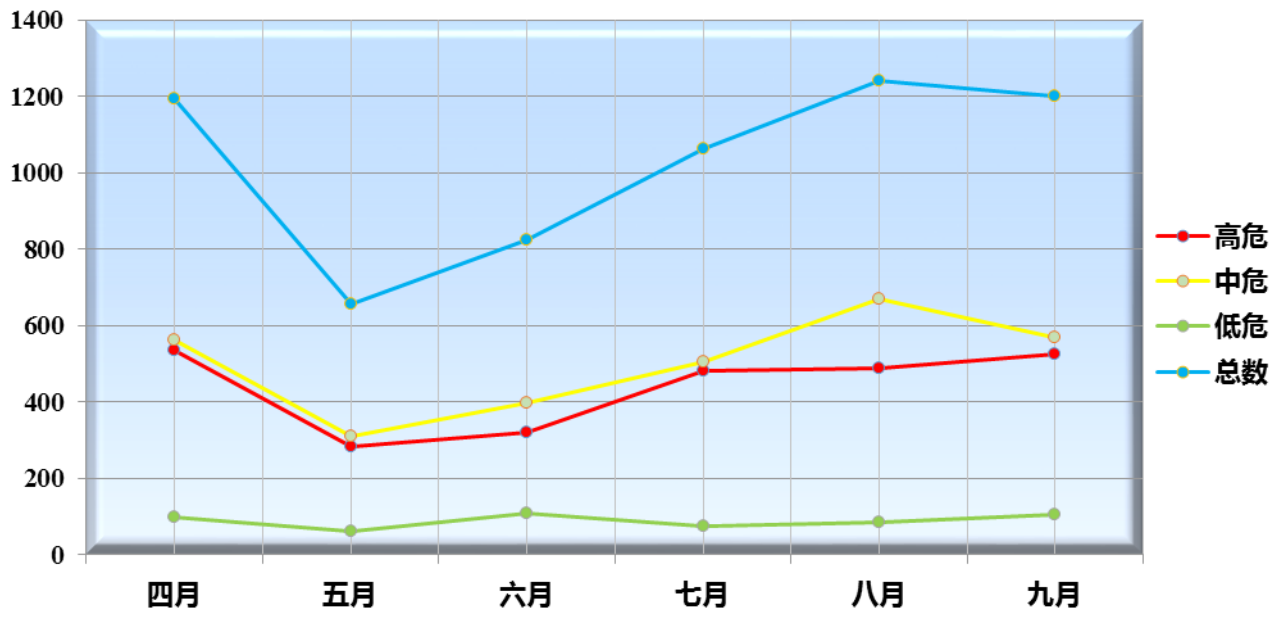

图 1-1 2017 年 4 月-2017 年 9 月漏洞新增数量趋势

二、 漏洞类型分布

2017 年 9 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 22.83%。值得关注的还有跨站脚本、信息泄露和权限许可和访问控制等常见漏洞类型。

表 1-2 2017 年 9 漏洞类型分布

类型	数量	比例
缓冲区溢出	274	22.83%
权限许可和访问控制	79	6.58%
信息泄露	82	6.83%
输入验证	48	4.00%
跨站脚本	112	9.33%
资源管理错误	31	2.58%
未知	314	26.17%
跨站请求伪造	21	1.75%
SQL 注入	57	4.75%
数字错误	13	1.08%
其他	169	14.08%

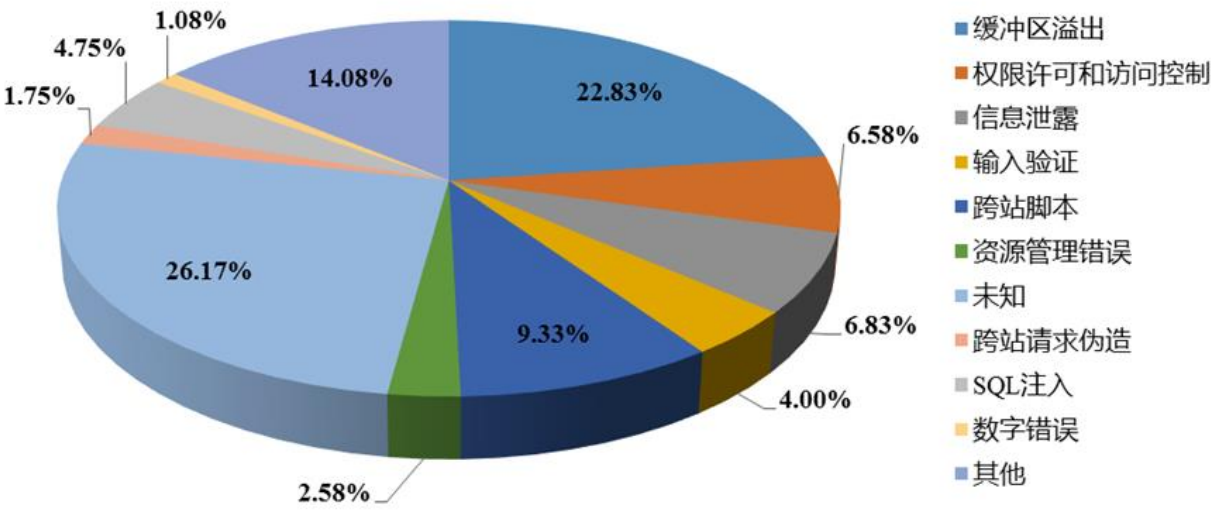

图 1-2 2017 年 9 月漏洞类型占比

三、 高危漏洞实例

(一)Struts2 REST 插件远程代码执行漏洞(S2-052)

CVE 编号：CVE-2017-9805

CNNVD 编号：CNNVD-201706-914

发布时间：2017-9

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Struts 2.5 - Struts 2.5.12

Struts 2.1.2 - Struts 2.3.33

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。从 Struts 2.1 开始，新增了 struts2-rest-plugin 插件，允许 Struts 2 应用对外提供 REST 服务。struts2-rest-plugin 插件也无需使用 XML 进行配置管理。该 REST 插件默认支持 XHTML、XML 和 JSON 三种形式的数据。

S2-052 漏洞是由于 struts2-rest-plugin 插件使用的 XStream Handle 处理器中的 toObject() 方法存在问题，在处理 XMLpayloads 过程中，未对传入的任何代码进行正确过滤，在使用 XStream 反序列化转换成对象时，可能会导致任意代码执行。

攻击者可以利用此漏洞对远程主机进行执行代码，危害系统安全。

修补建议：在不使用时删除 Struts REST 插件，或仅限于服务器普通页面和 JSONs：<constant name=”struts.action.extension”value=”xhtml,,json” />。建议尽快升级到 2.5.13 版本或者 2.3.34 版本，目前厂商已经发布了升级补丁，补丁获取链接：

https://struts.apache.org/docs/s2-052.html

(二)Tomcat 远程代码执行漏洞

CVE 编号：CVE-2017-12615

CNNVD 编号：CNNVD-201709-899

发布时间：2017-9

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Apache Tomcat 7.0.0 - 7.0.80

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。

该漏洞的利用前提是在 Windows 环境下，将 Tomcat 的 conf/web.xml 文件中的 readonly 设置为 false ,即启用 HTTP PUT 请求方法 ,攻击者利用该漏洞通过发送精心构造的恶意请求，向服务器上传恶意 JSP 文件，达到在服务器上执行任意代码的目的。

攻击者可以利用此漏洞对远程主机进行执行代码，危害系统安全。

修补建议：配置 readonly 值为 True 或注释参数，禁用 PUT 方法并重启 Tomcat。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://tomcat.apache.org/download-70.cgi?spm=5176.bbsr536282.0.0.1iXJnD&file=download-70.cgi

(三) Java Spring Data REST 远程代码执行漏洞

CVE 编号：CVE-2017-8046

CNNVD 编号：CNNVD-201704-1106

发布时间：2017-9

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Spring Data REST < 2.5.12, 2.6.7, 3.0 RC3

Spring Boot < 2.0.0M4

Spring Data release trains < Kay-RC3

漏洞描述：Spring 是 J2EE 应用程序框架，是轻量级的 IoC 和 AOP 的容器框架。

该漏洞与 Spring-data-rest 服务器在处理 PATCH 请求时有关。攻击者通过将精心构造的恶意 PATCH 请求提交给 spring-data-rest 服务器，提交的 JSON 数据中存在 SPEL 表达式可以执行任意的 Java 代码。

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。

修补建议：升级到版本 Spring Data REST2.5.12, 2.6.7, 3.0 RC3、Spring Boot 2.0.0.M4、Spring Data release train Kay-RC3。目前厂商已经发布了升级补丁，补丁获取链接：

https://pivotal.io/security/cve-2017-8046

(四)Joomla! LDAP 注入漏洞

CVE 编号：CVE-2017-14596

CNNVD 编号：CNNVD-201709-882

发布时间：2017-9

危险等级：☆☆☆

漏洞类型：注入

受影响软件：

Joomla! 1.5-3.7.5

漏洞描述：Joomla!是 Open SourceMatters 团队开发的一套开源的使用 PHP 语言和 MySQL 数据库的内容管理系统(CMS) ,是网站的一个基础管理平台。可以在 Linux、Windows、MacOSX 等各种不同的平台上执行。

该漏洞的利用条件是，Joomla!配置使用 LDAP 进行身份验证。LDAP 认证插件中的转义不足，导致远程攻击者可以提取到使用 LDAP 服务器的所有身份验证凭据（用户名和密码），利用获取到的信息可以登录到管理员控制面板。

攻击者可以利用此漏洞获取管理员账户密码，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://developer.joomla.org/security-centre/711-20170902-core-ldap-information-disclosure

(五)Tomcat 信息泄露漏洞

CVE 编号：CVE-2017-12616

CNNVD 编号：CNNVD-201709-898

发布时间：2017-9

危险等级：☆☆☆

漏洞类型：信息泄露

受影响软件：

Apache Tomcat 7.0.0 - 7.0.80

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。

该漏洞的利用前提条件是 Tomcat 的 server.xml 文件配置了 VirtualDirContext 参数，默认情况下是没有配置 VirtualDirContext 参数的。当使用了 VirtualDirContext 参数时，攻击者利用该漏洞通过发送精心构造的恶意请求，达到获取到服务器上 JSP 文件的源代码的目的。

攻击者可以利用此漏洞，获取敏感信息，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://tomcat.apache.org/download-70.cgi?spm=5176.bbsr536282.0.0.1iXJnD&file=download-70.cgi

四、 本月安全要闻

(一)流行音乐媒体 Vevo 服务器遭黑客组织 OurMine 入侵，致使逾 3.1 TB 内部文件与视频在线泄露

HackerNews.cc 9 月 16 日消息，流行音乐媒体 Vevo 服务器遭黑客组织 OurMine 入侵，致使逾 3.1 TB 内部文件与视频在线泄露，其中包括 90 多名不同艺术家私人档案（例如：泰勒斯威夫特、贾斯汀比伯、凯蒂佩里、小甜甜布兰妮、麦当娜等）、公司社交媒体战略备忘录、英国 Vevo 办公室禁用报警系统说明、电商营销信息、每周音乐排行榜等内部文件。

OurMine 是一个自称安全黑客的团队，他们经常通过侵入一些大咖的社交网络账号给自己打广告。就在上个月他们还曾窃取过 HBO 和《权力的游戏》的社交媒体账号（注：窃取 1.5TB 数据的并非 OurMine 团队），但 OurMine 宣称他们仅仅“在测试 HBO 系统的安全性能”。不过，他们此前主要攻击的目标是科技圈内的 CEO、企业与新闻网站，旨在通过漏洞入侵社交账号后兜售自家安全服务。

黑客组织 OurMine 在窃取 Vevo 大量数据后于 9 月 14 日通知公司，但遭到雇员怀疑与亵渎。不过，尽管 OurMine 已泄露大量数据，但他们还是在官网声称：“如果 Vevo 代表主动与我们取得联系，我们会立即删除数据”。最终，OurMine 删除了在线数据。随后，Vevo 在一份声明中证实并表示此次泄露事件主要是通过网络钓鱼攻击的结果。目前，Vevo 已妥善解决这个问题并正在加大调查力度，以确保公司信息安全。

友情链接：http://hackernews.cc/archives/14777

(二)美国信用机构 Equifax 遭黑客入侵，1.43 亿用户记录在线泄露

美国共有 3 家大型老牌征信企业，Equifax 正是其中之一，它掌管 8 亿公民的信用、保险记录，如果黑客想窃取数据，Equifax 往往会成为攻击目标。Equifax 表示，泄露从 5 月中旬开始，直至 7 月 29 日公司才察觉。

目前，犯罪分子已获取公民个人信息，其中包括姓名、住址、出生日期、社会保障号，有时还会包含驾照信息。据悉，黑客可以通过访问公民信息，为受害用户创建帐户或接管帐户。此外，在美国泄露的信息还包括 20.9 万人的信用卡卡号、18.2 万人的特定争议文件。

为了应对危机，Equifax 开通一个向所有美国公民提供 1 年免费保护的服务网站，可以对公民信贷进行监控，以防止身份被窃，只是暂时还不知道是否实用。由于受害者众多，泄露的信息也很多，这可能是近年来最大的泄露事故。之前雅虎虽然泄露了 10 亿帐户的信息，不过里面没有包含社会保障号和驾照号码。

安全专家表示，Equifax 遭遇黑客入侵对广大消费者是一个警示，提醒大众要特别注意个人信息在互联网泄露的风险。

“（被入侵的用户数据）是庞大的，”网络安全公司 Iboss 首席执行官保罗·马蒂尼（Paul Martini）在接受彭博社采访时表示。“这超出了我们以往见过的任何其他数据漏洞——不仅入侵的规模，还有被入侵的数据库中的数据类型。”

《每日经济新闻》记者注意到，Equifax 还特意建立了一个网站（www.equifaxsecurity2017.com），以便让消费者可以登陆查询他们的个人信息是否被入侵。此外，Equifax 还提供免费的信用文件监控和身份盗窃保护。

“在今年 5 月中旬至 7 月间 犯罪分子利用了美国网站的应用程序漏洞来获取某些文件，”Equifax 表示。

美国联邦调查局（FBI）在一份声明中表示，已经知悉这起黑客事件，并将“在适当的情况下追踪事态进展”。

友情链接：http://tech.qq.com/a/20170908/083717.htm

(三)瑞典最大网络托管公司 Loopia 遭黑客入侵，引发数十万客户敏感数据泄露

据外媒报道，瑞典最大网络托管公司 Loopia 数据库遭黑客入侵，引发数十万客户敏感数据泄露。

随后，Loopia 公司发表了声明，确认黑客于 8 月 22 日时入侵了公司的数据库系统，并在线访问了部分客户的敏感信息，其中包括客户的个人资料、联系方式、以及 Loopia Kundzon 登录密码（哈希加密），不过，客户的信用卡支付信息和电子邮件等服务并未遭受影响。

Loopia 目前是瑞典最大的网络托管公司之一，其拥有数十万的客户群体，其中有大部分是来自瑞典首都斯德哥尔摩、卡罗琳卡研究所、以及瑞典西海岸中心地区 Västra Götaland，其中卡罗琳卡研究所更是诺贝尔奖委员会所在地。

由此可见，此次受到影响的客户群体并不是一般网络托管公司的常规用户，一旦出现敏感数据泄露，其影响是很难估量的。

据了解，Loopia 公司在确保系统安全后，已于上个月 25 日下发通知，建议用户重置系统密码并更新个人信息，以避免黑客再次发动攻击行为。此次黑客入侵 Loopia 公司数据库后，以“拖库”的形式泄露了数以十万计的客户敏感信息。而所谓的“拖库”，就是指黑客通过各种手段成功入侵目标数据库后，窃取了数据库并导出的一种泄密方式，根据目标数据库存储内容类别、规模的多少，产生的危害各不相同。

友情链接：http://www.lwd3699.com/anquan/946.html

(四)美国 TigerSwan 因第三方 AWS 漏洞泄露数千份敏感简历，或含美驻印尼大使、中情局前员工信息

安全公司 UpGuard 网络风险研究人员 Chris Vickery 近期发现第三方招聘公司 TalentPen 因安全疏忽，导致逾 9,400 份美国私人安全公司 TigerSwan 的雇佣简历在未受保护的 Amazon Web Services（AWS）存储服务器上泄露，其中包括员工住址、电话号码、电子邮件地址、驾驶执照与护照号码以及社会保险号码等敏感信息。

相关调查显示，这些雇佣简历在线暴露了 TigerSwan 自 2008 年成立来所有员工资料，其中包括许多加入公司且目前仍在伊拉克战争后期、索契奥运会以及北达科他州管道参加抗议活动提供安全支持的员工信息。此外，虽然多数简历申请人以美国退伍军人为主，但其中还是包含几份据称是与美国部队、政府机构合作的伊拉克与阿富汗雇佣简历。然而，UpGuard 还在发表的博客文章中宣称，上述泄露的雇佣简历还包括前美国驻印尼大使的联络资料，以及中情局秘密服务的前任主席敏感信息，其中许多人具备最高机密的安全许可。研究人员表示，此类数据在国外情报机构中会受到“高度关注”。

亚马逊已于 8 月 24 日关闭 TalentPen 服务器，随后 TigerSwan 发表声明宣称：“公司已通知受害用户数据泄露的情况以防黑客展开网络钓鱼攻击。我们认真考虑到 TalentPen 未能确保公司信息安全并对员工造成不便表示遗憾。现今我们将与 TalentPen 终止合作并建立一台属于 TigerSwan 的安全站点，以便公司今后将雇佣简历传输至 TigerSwan 服务器。目前，Talent Pen 并未发表任何评论。

友情链接：http://wemedia.ifeng.com/28351877/wemedia.shtml

(五)欧洲与北美数十家能源机构，遭俄罗斯黑客组织“蜻蜓”针对性网络攻击

据外媒报道，赛门铁克于 9 月 6 日发布安全报告，宣称欧洲与北美能源部门似乎正面临俄罗斯黑客组织“ 蜻蜓（Dragonfly）”全面攻击风险。调查显示，目前已有数十家境外基础设施遭到黑客针对性攻击，其中多数位于美国。

黑客组织“ 蜻蜓 ”（又名：“Energetic Bear”或“Crouching Yeti”）自 2011 年以来一直处于活跃状态，但研究人员表示该组织从 2014 年被曝光后隐藏近两年，随后于 2015 年年底通过部署大规模网络钓鱼邮件复苏并开始展开新一轮攻击活动。据悉，黑客组织“ 蜻蜓 ”此前曾依赖暗网中的自定义恶意软件感染目标系统，窃取受害用户重要数据。

调查显示，黑客组织“蜻蜓”于 2016 – 2017 年进行了一起以“ 能源企业发展 ”为主题的恶意电子邮件分发活动，旨在窃取用户敏感数据。今年，赛门铁克观察到，该组织使用了一款名为“ Phishery ”的工具包，而该工具包自去年以来一直于暗网公开发售并允许黑客在用户不知情下入侵目标系统。近期，美国、土耳其与瑞士等多国基础设施疑似遭该黑客组织攻击。

据悉，虽然黑客现已成功控制多数受害系统，但研究人员尚不清楚攻击者最终目标或真正意图。不过，根据黑客长久的控制操作可以推测，攻击者具备政治动机，与早前乌克兰电厂攻击活动存在异曲同工之处，尽管二者之间无明确关系。

友情链接：http://hackernews.cc/archives/14460

