迪普科技 2018 年 8 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 8 月份新增安全漏洞 938 个。比上月减少了 985 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 80 个，中危漏洞 661 个，低危漏洞 197 个，同比 2017 年 8 月 (漏洞总数 1242 个) 减少 24.48%。表 1-1 为 2018 年 3 月-2018 年 8 月漏洞危险等级统计。

表 1-1 2018 年 3 月-2018 年 8 月漏洞危险等级统计

	三月	四月	五月	六月	七月	八月
高危	**144**	**436**	**48**	**58**	**10**	**80**
中危	**277**	**313**	**65**	**115**	**320**	**661**
低危	**52**	**56**	**5**	**4**	**1593**	**197**
总数	**473**	**805**	**118**	**177**	**1923**	**938**

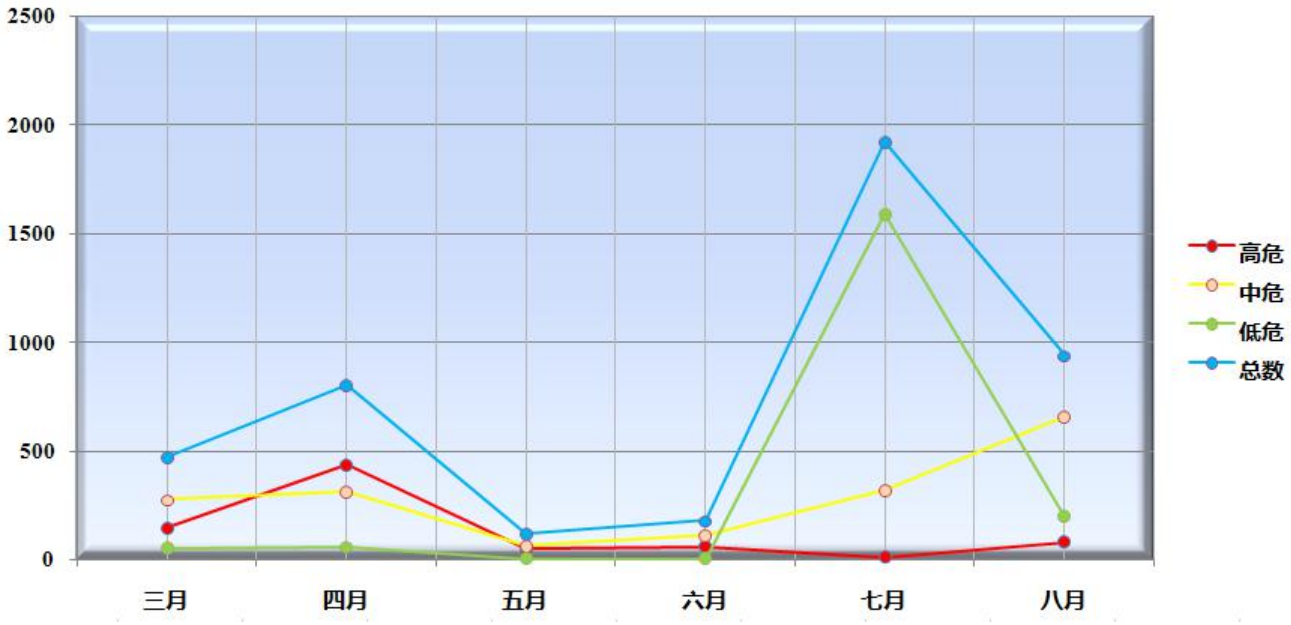

图 1-1 2018 年 3 月-2018 年 8 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 8 月份新增的漏洞类型分布如表 1-2 所示。其中跨站脚本，占 11.33%。值得关注的还有跨站请求伪造、信息泄露等常见漏洞类型。

表 1-2 2018 年 8 月漏洞类型分布

类型	数量	比例
未知	807	70.85%
跨站脚本	129	11.33%
跨站请求伪造	43	3.78%
信息泄露	41	3.60%
SQL 注入	28	2.46%
权限许可和访问控制	25	2.19%
路径遍历	19	1.67%
输入验证	9	0.79%
数字错误	7	0.61%
缓冲区溢出	4	0.35%
其他	27	2.37%

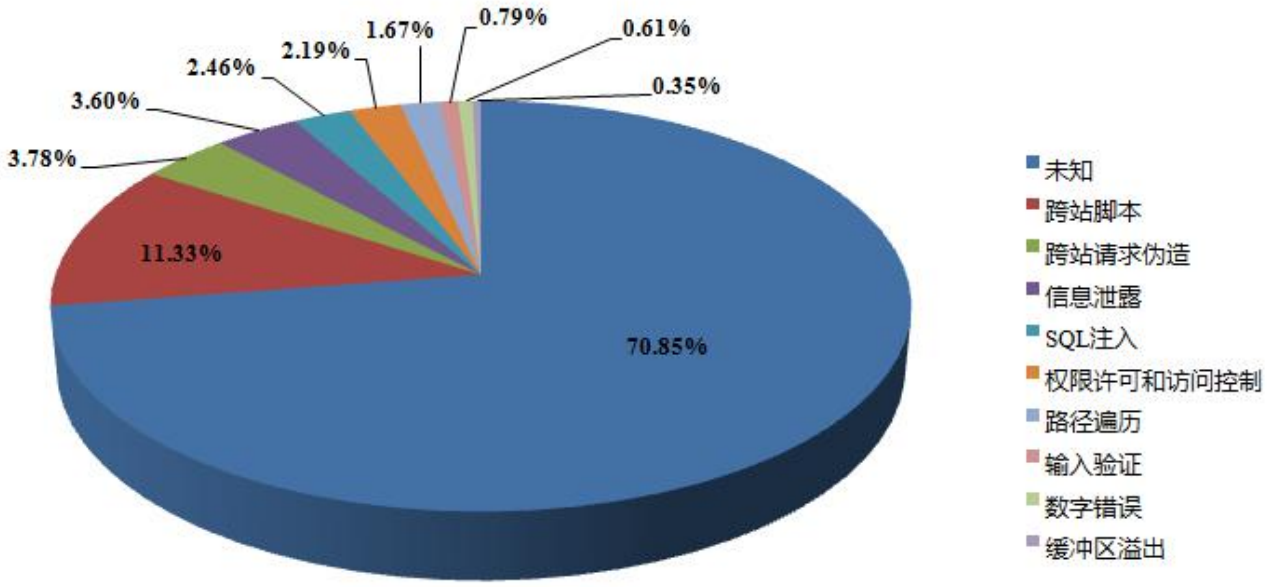

图 1-2 2018 年 8 月漏洞类型占比

三、 高危漏洞实例

(一) Struts2 S2-057 远程命令执行漏洞

CVE 编号：CVE-2018-11776

CNNVD 编号：CNNVD-201808-740

发布时间：2018-08

危险等级：☆☆☆☆☆

漏洞类型：命令执行

受影响软件：

Struts 2.3 – Struts 2.3.34

Struts 2.5 – Struts 2.5.16

漏洞描述：Apache Struts2 是美国 Apache 软件基金维护的一个开源项目，其最初被称为 WebWork2，是采用 Java Web 构建的网站系统常用的一款框架，可用于快速创建企业级 Web 应用程序。在使用 Struts2 开发的 Web 应用程序中，xml 配置文件决定了容器中的 HTTP 元素如何进行处理。

当底层的 xml 配置文件中未设置 namespace 值，并且上层的 action 配置中没有使用或者使用了通配符的 namespace 配置，可能会导致远程命令执行漏洞（即 RCE 漏洞）。同时，当使用了没有设置值和 action 的 url 标签，并且其上层的 action 配置中没有使用或者使用了通配符的 namespace 配置，也可能会导致该漏洞的发生。

攻击者可以利用该漏洞执行任意代码，危害系统安全。

修补建议：升级 Struts 版本到 2.3.35 或 2.5.17 以规避该风险，获取链接：

http://struts.apache.org/download.cgi

（二） WordPress 任意文件上传漏洞

CVE 编号：CVE-2018-14028

CNNVD 编号：CNNVD-201808-295

发布时间：2018-08

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

WordPress 4.9.7

漏洞描述：WordPress 是一种使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。在国际上广泛使用了，可以兼容自开发的插件。功能强大，应用广泛。

该漏洞是由于没有对上传的文件进行正确的验证过滤，攻击者可以利用该漏洞通过管理区域上传的插件上传恶意 PHP 文件。上传 PHP 文件后，该文件会被保留在 wp-content/uploads 目录下，攻击者可以执行该恶意文件。

攻击者可以利用该漏洞上传并执行恶意 PHP 文件，危害系统安全。

修补建议：目前厂商还未发布补丁，厂商链接：

https://github.com/rastating/wordpress-exploit-framework/pull/52

(三) PHP 拒绝服务漏洞

CVE 编号：CVE-2018-14851

CNNVD 编号：CNNVD-201808-064

发布时间：2018-08

危险等级：☆☆☆

漏洞类型：拒绝服务

受影响软件：

PHP < 5.6.37

PHP 7.0.x < 7.0.31

PHP 7.1.x < 7.1.20

PHP 7.2.x < 7.2.8

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/exif/exif.c 文件的 exif_process_IFD_in_MAKERNOTE 有关。攻击者可以利用该漏洞通过精心设计的 JPEG 文件进行越界读取，导致应用程序崩溃，造成拒绝服务攻击。

攻击者可以利用该漏洞造成拒绝服务攻击，危害系统安全。

修补建议：应用补丁，补丁获取链接：

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

(四) Joomla!文件上传漏洞

CVE 编号：CVE-2018-15882

CNNVD 编号：CNNVD-201808-932

发布时间：2018-08

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

Joomla! < 3.8.12

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。

该漏洞是由于 InputFilter 没有进行正确的过滤检测。攻击者可以利用该漏洞通过 phar 文件绕过上传过滤器，上传恶意文件，从而控制服务器。

攻击者可以利用该漏洞上传并执行恶意文件，危害系统安全。

修补建议：应用补丁，获取链接：

https://developer.joomla.org/security-centre/743-20180801-core-hardening-the-inputfilter-for-phar-stubs.html

(五) OpenSSH 用户枚举漏洞

CVE 编号：CVE-2018-15919

CNNVD 编号：CNNVD-201808-902

发布时间：2018-08

危险等级：☆☆

漏洞类型：设计缺陷

受影响软件：

OpenSSH <= 7.8

漏洞描述：OpenSSH 是使用 SSH 协议进行远程登录的首选连接工具。它加密所有流量，可有效消除窃听、连接劫持和其他网络攻击。OpenSSH 是 OpenBSD 的子项目。

该漏洞与 auth-gss2.c 有关，当使用了 GSS2 时，远程攻击者可以通过该漏洞检测目标系统上的用户是否存在。

攻击者可以利用该漏洞获取敏感信息，危害系统安全。

修补建议：目前厂商还未发布补丁，厂商链接：

https://www.openssh.com/

四、 本月安全要闻

（一） 华住 1.3 亿用户数据泄露，华住：已报警正核实

据 FreeBuf 报道，8 月 28 日早上 6 点，暗网中文论坛中出现一个帖子，声称售卖华住旗下所有酒店数据，数据标价 8 个比特币，约等于人民币 37 万人民币，数据泄露涉及到 1.3 亿人的个人信息及开房记录。而经过媒体报道之后，该发帖人称要减价至 1 比特币出售。

华住酒店集团旗下拥有“禧玥酒店”、“全季酒店”、“星程酒店”、“汉庭酒店”、“海友酒店”五个品牌，在全国 200 多个城市开设有 1900 多家门店。

数据包含汉庭酒店、美爵、禧玥、漫心、诺富特、美居、CitiGo、桔子、全季、星程、宜必思、怡莱、海友。

售卖的酒店数据分为三个部分：

1、华住官网注册资料，包括姓名、手机号、邮箱、身份证号、登录密码等，共 53G，大约 1.23 亿条记录；

2、酒店入住登记身份信息，包括姓名、身份证号、家庭住址、生日、内部 ID 号，共 22.3G，约 1.3 亿人身份证信息；

3、酒店开房记录，包括内部 id 号，同房间关联号、姓名、卡号、手机号、邮箱、入住时间、离开时间、酒店 id 号、房间号、消费金额等，共 66.2G，约 2.4 亿条记录。

紫豹科技风险监控平台情报专家通过技术手段验证了这批数据的真伪。据悉，疑似华住公司程序员将数据库连接方式上传至 github 导致其泄露，目前还无法完全得知到细节。

据威胁猎人数据验证结果：从测试数据结果来看，最低的住客年龄在 95 年，最近离店时间是 8 月 13 日。从数据交叉验证来看，可以排除是卖家用老数据欺诈买家的情况，数据

绝大部分为新泄露数据，而非老数据混杂售卖。基于此，该份数据的真实性非常高，此次的数据泄露也可能成为近 5 年内国内最大最严重的个人信息泄露事件。

早在 2013 年，汉庭等酒店就出现过数据泄露，当时是因为酒店所使用的 Wi-Fi 管理和认证管理系统存在漏洞，数据传输过程并未加密，导致数据泄漏。此次数据被拖库的原因尚不清楚，华住官方暂无回应。

友情链接：http://hackernews.cc/archives/23996

（二） 遭黑客入侵，美社交新闻网站 Reddit 数据再泄露

新浪科技讯，北京时间 8 月 2 日早间消息，美国社交新闻网站 Reddit 周三宣布，该公司的几个系统遭到黑客入侵，导致一些用户数据被盗，其中包括用户目前使用的电子邮箱以及 2007 年的一份包含旧加密密码的数据库备份。

Reddit 称，黑客获取了旧数据库备份的一个副本，其中包含了早期 Reddit 用户数据，时间跨度从 2005 年该网站成立到 2007 年 5 月。

“虽然这是一次严重的攻击，但攻击者并没有获得 Reddit 系统的写入权限。他们获得的是部分系统的只读权限，其中包含了备份数据、源代码和其他日志。”Reddit 创始工程师克里斯多夫·斯洛维（Christopher Slowe）写道。

斯洛维表示，Reddit 今年 6 月 19 日发现，攻击者在 6 月 14 日至 6 月 18 日期间入侵了该公司几名员工的帐号。

Reddit 表示，此次攻击是通过拦截员工的短信实现的，该短信中包含了一次性登录码。该公司还补充道，他们已经将此事通知受影响的用户。

斯洛维表示，该公司大约在 3 个月前聘请了第一位安全主管，“他目前还没有退出。”

友情链接：http://hackernews.cc/archives/23715

（三） T-Mobile 遭黑客入侵，200 万用户个人数据被盗

周四晚间，T-Mobile 披露了一起数据泄露事件，黑客窃取了 200 万用户的部分个人数据。该公司表示，在此次短暂的入侵中，黑客窃取了部分用户数据，包括姓名、电子邮件地址、帐号和其他账单信息。好消息是他们并未获取信用卡和社保号码。

T-Mobile 在声明中表示，其网络安全团队于 8 月 20 日（星期一）检测到“未经授权访问某些信息”的行为。

该公司网站上发表的声明称：“我们的网络安全团队发现并阻止了对包括您的信息在内的某些未经授权信息的访问，我们迅速向当局报告了此事。您的财务数据（包括信用卡信息）、社保号码以及密码并没有被泄露。但是，关于您的部分个人信息可能已被曝光，其中可能包含以下一项或多项信息：姓名、帐单编码、电话号码、电子邮件地址、帐号和帐户类型（预付或邮资）等。”

T-mobile 公司的一位发言人表示，在其 7700 万客户中，受到这一漏洞影响的客户占比“大约”或“略低于”3%。这位发言人在一条短信中提到：“幸运的是，受害者数量并不大。”但她拒绝透露确切的数字。

这位发言人补充道，这起“事件”发生在 8 月 20 日凌晨，一家国际集团的黑客通过 API 访问该公司服务器，该 API 不包含任何财务信息或其他敏感的数据。随后，在入侵的同一天，网络安全团队就监测到了这一漏洞。

该发言人说：“我们的团队很快发现并阻止了他们的潜在行为。”但她拒绝透露此次攻击的细节，公司方面对黑客的身份也一无所知。

该公司还在声明中表示：“所有受影响的用户已经或将很快收到通知。如果您没有收到通知，意味着您的帐户并未受此事件影响。”T-Mobile 同时鼓励相关用户拨打 611 与客服联系。

当外媒就该公司的措辞进行采访时，其发言人回应称：“我们做出上述声明的原因是，这些‘密码’均未受到损害，它们被加密了。”

该发言人拒绝详述这些密码的加密方式，也拒绝具体说明其所使用的散列算法（hashing algorithm）。在该数据泄露事件曝光的几个小时后，安全研究人员 Nicholas Ceraolo 表示，泄露的数据远超 T-Mobile 所披露的数据。该研究人员分享了一份疑似泄密数据的样本，其中包含一个名为“用户密码”的字段，与密码加密表示的散列（Hash）非常相似。（Ceraolo 表示自己并未受到黑客攻击，而是从一位“共同好友”那里获得了该份样本。）

友情链接：http://www.hackbase.com/portal.php?mod=view&aid=234934&page=1&

(四) 黑客组织从 28 个国家盗取印度 Cosmos 银行 1350 万美元

据报道，朝鲜著名黑客团伙 Lazarus 针对印度 Cosmos 银行展开复杂攻击进而谋财。

已发生的网络犯罪活动与朝鲜 Lazarus 组织有关——通过 28 个国家的 ATM 从印度一家银行盗得 1350 万美元。该攻击案发前几天，FBI 才刚刚警告过即将发生针对被黑银行的“取现”攻击。

据报道，印度 Cosmos 的合作银行遭受的这次攻击，攻击者能够绕过该行 ATM 交易系统上的安全措施，进行操作。该犯罪团伙散布在世界各地，利用 ATM 和克隆卡从攻击中获利。Cosmos 的 SWIFT 国际支付系统似乎同时被黑。

Cosmos 银行总裁 Milind Kale 承认，仅上周末，8 月 11 到 13 号之间，就发生了约 1.2 万起非法交易。2 天之内，黑客从 28 个国家的各型 ATM 上取出了 7.8 亿卢比(1110 万美元)，包括加拿大、香港和印度的一部分 ATM，另有 2500 万卢比(35.6 万美元)是从印度取出的。

据《印度经济时报》报道，8 月 13 号，攻击者还利用该行被黑的 SWIFT 国际支付系统，转账了 1.392 亿卢比(200 万美元)到一家香港银行。目前为止，该行总计损失了 1350 万美元，而鉴于系统被黑的程度，该数字还有可能继续上升。

《印度经济时报》描述称，黑客侵入了 ATM 交易机的服务器系统的防火墙，然后设置了代理服务器，用该虚假/代理服务器进行授权交易。也就是说，ATM 在攻击者控制下，不去检查银行卡是否真实就开始吐钱。

据独立安全记者布莱恩·克雷布斯报道，FBI 在周五就曾发出过相关警告。FBI 的警告写道：“网络罪犯通常会将被盗数据发送给共犯，由共犯将数据写入可重用磁条卡，比如零售店售卖的礼品卡，借此创建合法支付卡的虚假副本。”到了预定的时间，共犯便会用这些假卡从 ATM 取出被盗账户中的资金。

Cosmos 银行总裁急于向客户保证该行账户是安全的：“我们的安全系统并未被黑，今年 7 月刚刚接受过印度央行(印度储备银行(RBI))的审查，是安全的。”他表示：“在注意到多起不正常突发高额交易后，我行关闭了服务器和所有网上银行应用。”

这些交易发生在 2 小时 13 分钟内，范围涉及 28 个国家。攻击者用克隆卡取出每笔 100 美元到 2500 美元的资金。正是 RBI 通告的 Cosmos 银行存在异常交易活动。

Lazarus 组织一直以来都是全球多起 SWIFT 支付系统攻击案的背锅侠。最著名的案例就是它曾试图从孟加拉央行转账 9.51 亿美元。只不过，由于一个低级拼写错误被处理其中一起交易的代理银行职员发现，整个攻击活动才被及时阻止，但仍有部分款项没能追回。

友情链接：http://www.hackbase.com/article-229371-1.html

（五） 俄罗斯 400 多家工业公司遭遇鱼叉式网络钓鱼攻击

卡巴斯基实验室 ICS CERT 的研究人员在本周三（8 月 1 日）发表的一篇博文中指出，该团队发现了一系列带有恶意附件的网络钓鱼电子邮件，主要针对的是与工业生产相关的俄罗斯公司和机构。从主题和内容上来看，这些电子邮件极具针对性。攻击者将这些电子邮件伪装成合法的商业报价，并且电子邮件内容与其目标所进行的工作极具相关性。

研究人员表示，从他们收集到的数据来看，这一系列攻击开始于 2017 年 11 月，并且目前仍处于继续进行之中。值得注意的是，早在 2015 年就已经有类似攻击的记录。

根据卡巴斯基实验室提供的数据我们可以看出，大约有 400 家与工业生产相关的公司成为了此次攻击的目标，这包括制造业、石油和天然气、冶金、工程、能源、建筑、采矿以及物流等。在 2017 年 10 月到 2018 年 6 月期间，大约有 800 名在这些公司工作的员工遭到了攻击。

根据研究人员的说法，在这些攻击中使用的恶意软件安装了合法的远程管理软件——TeamViewer 或 Remote Manipulator System/Remote Utilities（RMS）。这使得攻击者能够远程控制受感染的系统。另外，攻击者还使用了各种技术来掩盖安装在系统中恶意软件的感染和执行。

根据现有的数据来看，攻击者的主要目标是从目标公司的帐户中窃取资金。当攻击者连接到受害者的计算机时，他们会搜索并分析目标公司的采购文件，以及该公司所使用的财务和会计软件。在此之后，攻击者会寻找各种方法来实施财务欺诈，例如伪造用于付款的银行详细信息。

此外，攻击者还使用了多种恶意软件来窃取数据，这包括 Babylon RAT、Betabot/Neurevt、AZORult stealer、Hallaj PRO RAT。不仅如此，攻击者还在某些系统中还安装了另一款远程管理实用程序 RemoteUtilities（在某些系统中还发现了 Mimikatz 一款能够获取 Windows 密码的工具），它提供了比 RMS 或 TeamViewer 更强大的功能集来控制受感染的计算机。

卡巴斯基实验室认为，此次攻击背后的组织者很可能是一个犯罪集团，至少一部分成员对俄语十分熟悉。因为只有熟练掌握俄语的人才能够将网络钓鱼电子邮件的内容编写得极具迷惑性，并且对目标公司财务数据的修改也需要很好的俄语基础。

值得注意的是，攻击者还试图通过分析目标公司员工的通信来获取更多的信息。他们很可能是在利用这些电子邮件中的信息来准备新的攻击，而攻击的目标很可能就是与当前受害者企业存在合作关系的公司。卡巴斯基实验室表示，除了直接的经济损失之外，这些攻击还可能导致受害者企业遭遇敏感数据泄露。

友情链接：https://www.hackeye.net/securityevent/15423.aspx