迪普科技 2017 年 10 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 10 月份新增安全漏洞 795 个。比上月减少了 405 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 280 个，中危漏洞 433 个，低危漏洞 82 个，同比 2016 年 10 月（漏洞总数 590 个）增长 34.75%。表 1-1 为 2017 年 5 月-2017 年 10 月漏洞危险等级统计。

表 1-1 2017 年 5 月-2017 年 10 月漏洞危险等级统计

	五月	六月	七月	八月	九月	十月
高危	283	319	483	487	524	280
中危	312	398	506	669	569	433
低危	63	108	74	86	107	82
总数	658	825	1063	1242	1200	795

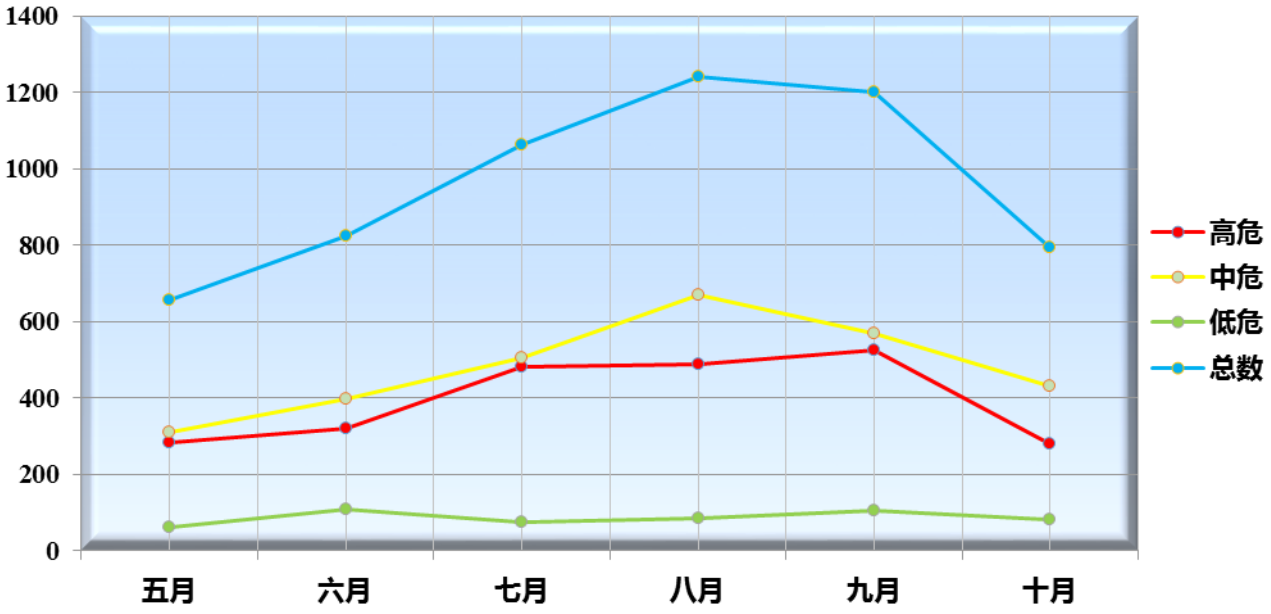

图 1-1 2017 年 5 月-2017 年 10 月漏洞新增数量趋势

二、 漏洞类型分布

2017 年 10 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 25.41%。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 10 漏洞类型分布

类型	数量	比例
缓冲区溢出	202	22.83%
权限许可和访问控制	50	6.58%
信息泄露	97	6.83%
输入验证	27	4.00%
跨站脚本	78	9.33%
资源管理错误	13	2.58%
未知	245	26.17%
跨站请求伪造	17	1.75%
SQL 注入	13	4.75%
路径遍历	6	1.08%
其他	47	14.08%

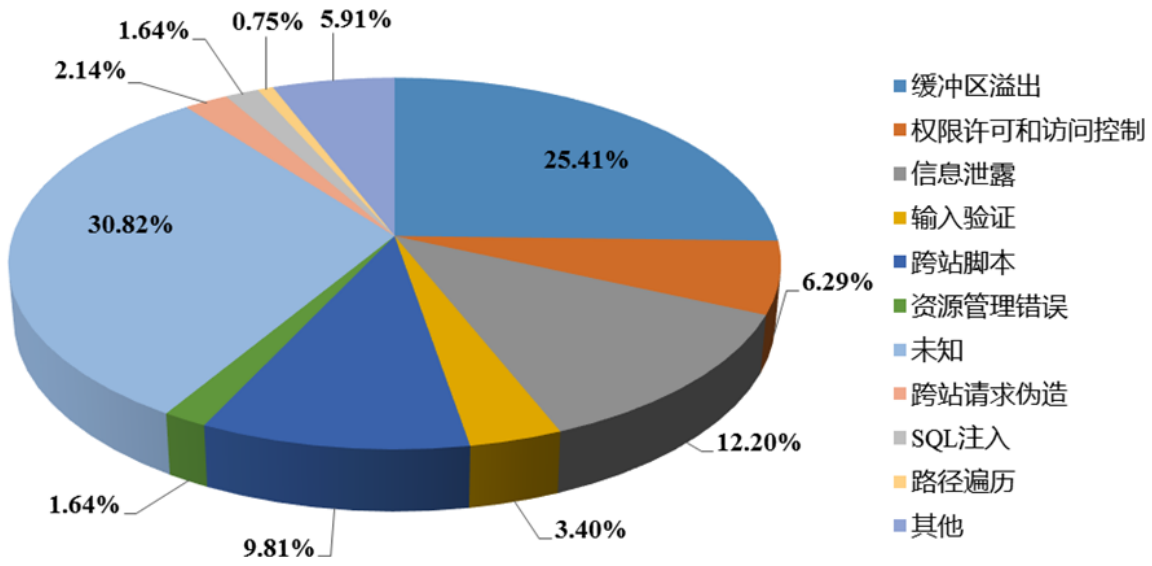

图 1-2 2017 年 10 月漏洞类型占比

三、 高危漏洞实例

(一)Microsoft Office 远程代码执行漏洞

CVE 编号：CVE-2017-11826

CNNVD 编号：CNNVD-201710-162

发布时间：2017-10

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Microsoft Word Automation Services

Word 2016

Word 2013 SP1

Word 2013 RT SP1

Word 2010 SP2

Word 2007 SP3

Share Point Enterprise Server 2016

Office Word Viewer

Office Web Apps Server 2013 SP1

Office Web Apps Server 2010 SP2

Office Online Server 2016

Office Compatibility Pack SP3

漏洞描述：Microsoft Office 是微软（Microsoft）公司开发的一套基于 Windows 操作系统的办公软件套件产品。

该漏洞是由于程序没有正确的处理内存中的对象。远程攻击者利用该漏洞通过特制的 RTF 格式文档发送给用户，如果用户使用受影响的 Microsoft Office 软件打开了该特制文件，就会使 Windows 操作系统被感染，植入木马后门，攻击者可以控制受影响的系统，窃取用户数据。

远程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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11826

(二)WordPress WPDB SQL 注入漏洞

CVE 编号：none

CNNVD 编号：none

发布时间：2017-10

危险等级：☆☆☆☆☆

漏洞类型：SQL 注入

受影响软件：

WordPress < 4.8.3

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。

该漏洞是由于对用户的输入没有进行正确的过滤，导致存在 SQL 注入漏洞。该漏洞与 $wpdb->prepare（ ）有关，利用精心构造的语句，可以进行 SQL 注入攻击，危害系统安全。

该漏洞会导致服务器的数据泄露，严重危害系统安全。

修补建议：尽快更新到最新稳定版本 4.8.3 版本，目前厂商已经发布了升级补丁，补丁获取链接：

https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/

(三) Oracle 远程安全漏洞

CVE 编号：CVE-2017-10151

CNNVD 编号：CNNVD-201710-1231

发布时间：2017-10

危险等级：☆☆☆☆

漏洞类型：设计缺陷

受影响软件：

Oracle Identity Manager 11.1.1.7

Oracle Identity Manager 11.1.1.9

Oracle Identity Manager 11.1.2.1.0

Oracle Identity Manager 11.1.2.2.0

Oracle Identity Manager 11.1.2.3.0

Oracle Identity Manager 12.2.1.3.0

漏洞描述：Oracle 是一个关系数据库管理系统，是目前世界上流行的关系数据库管理系统。Oracle Fusion Middleware 是一个中间件系列产品，Oracle Identity Manager Connector 是其中的一个资源适配器。

该漏洞与 Oracle 身份管理器组件有关，其中的 Default Account 子组件存在安全漏洞。该漏洞可以被未经身份验证的远程攻击者，通过 HTTP 远程访问，利用该漏洞对系统产生危害，可能会导致完全控制受影响的系统。

攻击者可以利用此漏洞完全控制受影响的系统，严重危害主机安全。

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://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10151-4016513.html

(四) Apache OpenOffice 远程代码执行漏洞

CVE 编号：CVE-2017-12608

CNNVD 编号：CNNVD-201708-310

发布时间：2017-10

危险等级：☆☆☆

漏洞类型：远程代码执行

受影响软件：

Apache OpenOffice <= 4.1.3

漏洞描述：Apache OpenOffice 是 Apache 软件基金会的一款开源免费的文字处理软件，在 Windows、Linux、Solaris 等操作系统上都能执行。

该漏洞与"WW8RStyle::ImportOldFormatStyles" 功能有关，存在一个可利用的越界写入漏洞。特制的恶意 doc 文件可能导致越界写入，使得内存损坏，导致任意代码执行。攻击者可以通过发送或者提供恶意文档文件来触发此漏洞。

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：

http://www.openoffice.org/download/index.html

(五) OpenSSH 'sftp-server.c' 远程安全绕过漏洞

CVE 编号：none

CNNVD 编号：none

发布时间：2017-10

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

OpenSSH < 7.6

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‘sftp-server.c’模块有关，是由于设计缺陷所导致的。攻击者可以利用该漏洞执行未授权动作，为下一步攻击制造条件。

攻击者可以利用此漏洞执行未授权动作，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.openssh.com/

四、 本月安全要闻

(一)暗网市场 Basetools 遭入侵，黑客以“将数据移交美国 FBI、国土安全部”为由勒索 5 万美金

据外媒报道，安全研究人员近期发现暗网市场 Basetools 遭黑客入侵并在线泄露了其数据库部分信息。黑客随后威胁暗网市场管理员支付 5 万美元赎金，否则就将其运营者身份以及相关数据移交至美国联邦调查局（FBI）、国土安全部（DHS）、司法部（DoJ）和其他机构。

Basetools 是一所地下交易市场，经常在俄语网络犯罪论坛发布广告，允许暗网供应商出售垃圾邮件工具、信用卡数据、黑客账户，以及其他东西。据称，该暗网市场号称拥有超过 15 万的用户，并提供逾 2 万种销售工具，以及 7*24 的服务支持。

安全专家表示，黑客在入侵 Basetools 数据库后兜售了一些工具，包括后门、shell 和 C-Panel 账户的登录凭证、托管在黑客攻击服务器上的垃圾邮件，以及此前其他互联网平台泄露的用户数据。消息显示，由于担心被泄露的工具可能会被其他网络犯罪分子用来发动恶意攻击，运营者在黑客泄露数据后已立即将网站下线。

虽然网络犯罪分子和敌对的暗网市场互相攻击并不是一种新现象，但此类攻击在多数情况下都是由经济动机推动。据研究人员介绍，AlphaBay 和 Hansa 两大最受欢迎的暗网市场于前段时间被查处关闭，从而导致网络犯罪事件于近期陷入了混乱和分散状况。

友情链接：http://hackernews.cc/archives/16272

(二)47GB 医疗数据库泄露：含 15 万患者姓名和检查结果

网络安全机构 Kromtech Security 信息专家近期披露，一份包含 47GB 医疗数据文件的 Amazon S3 云存储对象提供公开访问，包含多达 315,363 份 PDF 档案，疑似为来自医疗设备公司 Patient Home Monitoring 的医疗数据存储纪录遭破解泄露，涉及近 15 万患者的姓名、地址、医生和病例纪录以及周常血液检查结果等隐私信息。又是一起大规模的涉及公众隐私信息的泄露事件。

Kromtech Security 公司指出网站上的隐私相关页面，该公司保障患者拥有权利知晓谁访问了与其相关的医疗健康保密信息，以及以和目的访问。而这起大规模各种泄露事件无疑违反了这项隐私条例，也违背了美国 HIPAA 法案（健康保险携带和责任法案）。Kromtech 方面称它们在 9 月 29 日发现了该公司的相关文件被泄露，随后在 10 月 5 日以邮件形式通知了该公司的相关问题。但在 10 月 6 日，这份泄露数据库已经开启了公众访问，目前尚未消息披露谁破解并泄露了这份文件。

友情链接：http://www.cnbeta.com/articles/tech/659561.htm

(三)黑客攻击尼泊尔中央银行 SWIFT 系统，440 万美金的转账，得手 58 万

本月，尼泊尔最大的私营商业银行之一遭受了黑客攻击，导致攻击者通过 SWIFT 银行间信息服务机构发出欺诈性资金转账。

据报道，位于加德满都的 NIC 亚洲银行表示，攻击者在六其他国家（包括美国、英国、日本和新加坡） 发起了 440 万美元的欺诈性资金转帐。

但在发现可疑交易后，NIC 亚洲银行立即通知尼泊尔中央银行、尼泊尔国家银行，但最终只收回了 390 万美元，有 58 万美元已经被海外银行账户持有。无论是 NIC 亚洲银行还是 NRB，都没有立即回应对银行劫案和调查的置评请求。

但据报道，攻击事件发生在提哈尔，攻击时间是在排灯节期间，这是印度教和尼泊尔一个比较大的节日，为期五天。今年，该节日从 10 月 17 日至 10 月 21 日。

黑客攻击的目标是在渣打银行纽约和马什雷克银行纽约的往来账户，该账户用于外汇交易和贸易。在发现可疑交易后，NIC 亚洲银行委托毕马威印度进行数字鉴证审查，并与 NRB 和尼泊尔警方中央调查局（喜马拉雅通讯社）的报告进行了交流。但据报道，调查结果未能得出结论，无法判断盗窃是由外部袭击者还是内部盗窃造成的。尼泊尔警察局副总监卡尅告诉媒体。

NIC 亚洲银行的副首席执行官罗山（库马尔 Neupane）对印度通讯社说，该行在发现可疑交易后立即将 SWIFT 服务器离线。对尼泊尔中央银行发起的抢劫案的调查发现，在 NIC 亚洲银行 SWIFT 部门的六名员工使用了一台电脑，这意味着该计算机只用于 SWIFT 交易。目前，这六名雇员都已转入其他部门。

友情链接：http://toutiao.secjia.com/nepalese-banks-swift-server-hacked

(四)瑞典交通机构上周曾遭黑客 DDoS 攻击，致使订单 IT 系统宕机、列车延误

据外媒报道，瑞典三家交通机构的 IT 系统于 10 月 11 日、12 日分别遭到黑客 DDoS 攻击，导致官网服务掉线、列车运行延误。

调查显示，黑客于 10 月 11 日针对瑞典运输管理局（Trafikverket）展开 DDoS 攻击，导致该机构负责管理列车订单的 IT 系统瘫痪，以及电子邮件系统与网站宕机，从而影响了旅客预定或修改订单的情况。不过，该机构随后通过 Facebook 向旅客提供了有关情况的最新信息。

瑞典交通管理局的新闻通讯官员 Pär Aronsson 证实，机构多个 IT 系统受到黑客攻击，其中包括能够显示列车位置的驱动系统。不过，虽然部分问题还在调查，但多数系统仍可正常运行。此外，知情人士透露，黑客发动的 DDoS 攻击主要针对服务提供商 TDC 和 DGC，其目的是影响机构的正常运营。

起初，安全专家认为这仅仅是一次突发事件，但第二天，另一家政府机构——瑞典交通运输局（Transportstyrelsen），以及公共交通运营商 Västtrafik 的 IT 系统遭到类似 DDoS 攻击，短暂性的破坏了官网的机票预订应用和在线旅游计划。互联网提供商 DGC 的副首席执行官 Patrik Gylesjö 表示，这可能是一场恶作剧，或者有人想要试图调查瑞典交通机构的预防措施。

目前，安全专家很难将此次攻击归因于简单的信息盗窃行为，因为他们根据俄罗斯上月开展的“ 萨帕德 ” 军演推测，这更像是俄罗斯测试其网络能力，从而调查瑞典的交通基础设施情况。

友情链接：http://hackernews.cc/archives/15845

(五)澳国防承包商逾 30G 资料遭黑客窃取，涉及 F35、P-8 等战机机密信息

HackerNews.cc 10 月 11 日消息，澳大利亚网络安全中心（ACSC）近期发布了一份《2017 ACSC 安全威胁报告》，指出澳大利亚国防承包商的 F-35 联合攻击战斗机、P-8 波塞冬海上巡逻机、C-130 运输机、联合直接攻击弹药（JDAM）智能炸弹组件，以及多艘海军舰艇等 30 GB 的敏感数据于早前遭黑客“ Alf ”窃取。

据悉，该起黑客事件最早可追溯至 2016 年 7 月。不过，澳大利亚信号理事会（ASD）的监管机构于同年 11 月才发现黑客侵入国家国防承包商网络系统，并持续访问一段时间后窃取大量敏感数据。负责该案件的 ASD 应急主管 Mitchell Clarke 表示，国家机密信息受国际武器条例（ITAR）的限制，而该系统是美国设计用来控制国防与军事相关技术出口的网络系统，因此被盗信息并非军事机密。

调查显示，由于受害公司所有与 IT 相关的权限均由工作人员轮流负责且管理时长为九个月，员工流动几率极高，因此容易导致公司内部信息的泄露。此外，知情人士透露，ASD 经调查发现黑客“ Alf ”访问系统内部文件极其容易，因为该公司 IT 系统存在一处安全漏洞，即所有服务器均使用默认管理员登录 ID 与密码，从而允许黑客轻松破解后访问系统内部域控制器、远程桌面服务器，并发送电子邮件以及其他敏感信息。

然而，研究人员还发现公司所有服务器上既没有设置 DMZ 区防护，也没有常规的漏洞修补方案，让人着实担忧。最后，Clarke 在报告中强调，各企业理应加强系统补丁修复、更改设备默认密码，以便保护企业网络安全、减少黑客事件发生。

友情链接：http://hackernews.cc/archives/15706

