迪普科技 2017 年 12 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 12 月份新增安全漏洞 670 个。比上月减少了 12 个，与前 5 个月平均数量相比，安全漏洞数量小幅减少。本月新增的漏洞中，高危漏洞 392 个，中危漏洞 247 个，低危漏洞 31 个，同比 2016 年 12 月（漏洞总数 530 个）增长 26.42%。表 1-1 为 2017 年 7 月-2017 年 12 月漏洞危险等级统计。

表 1-1 2017 年 7 月-2017 年 12 月漏洞危险等级统计

	七月	八月	九月	十月	十一月	十二月
高危	483	487	524	280	282	392
中危	506	669	569	433	287	247
低危	74	86	107	82	89	31
总数	1063	1242	1200	795	658	670

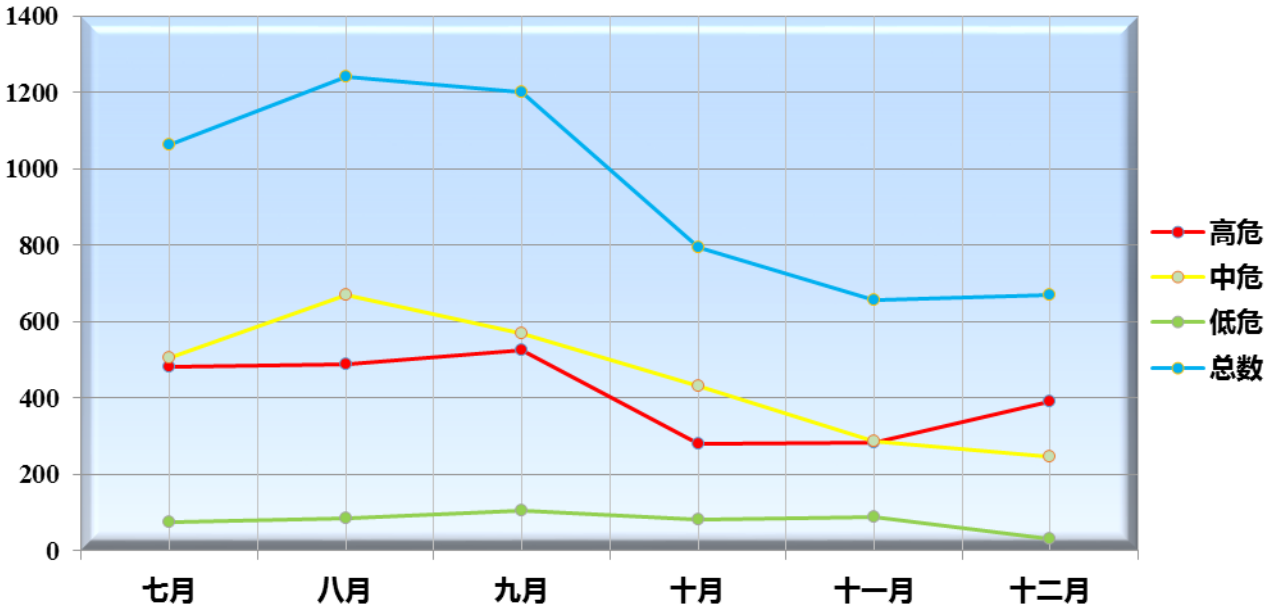

图 1-1 2017 年 7 月-2017 年 12 月漏洞新增数量趋势

二、 漏洞类型分布

2017 年 12 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 16.12%。值得关注的还有 SQL 注入、信息泄露和跨站脚本等常见漏洞类型。

表 1-2 2017 年 12 月漏洞类型分布

类型	数量	比例
缓冲区溢出	108	16.12%
权限许可和访问控制	49	7.31%
信息泄露	76	11.34%
输入验证	21	3.13%
跨站脚本	41	6.12%
资源管理错误	6	0.90%
未知	246	36.72%
竞争条件	9	1.34%
SQL 注入	83	12.39%
路径遍历	6	0.90%
其他	25	3.73%

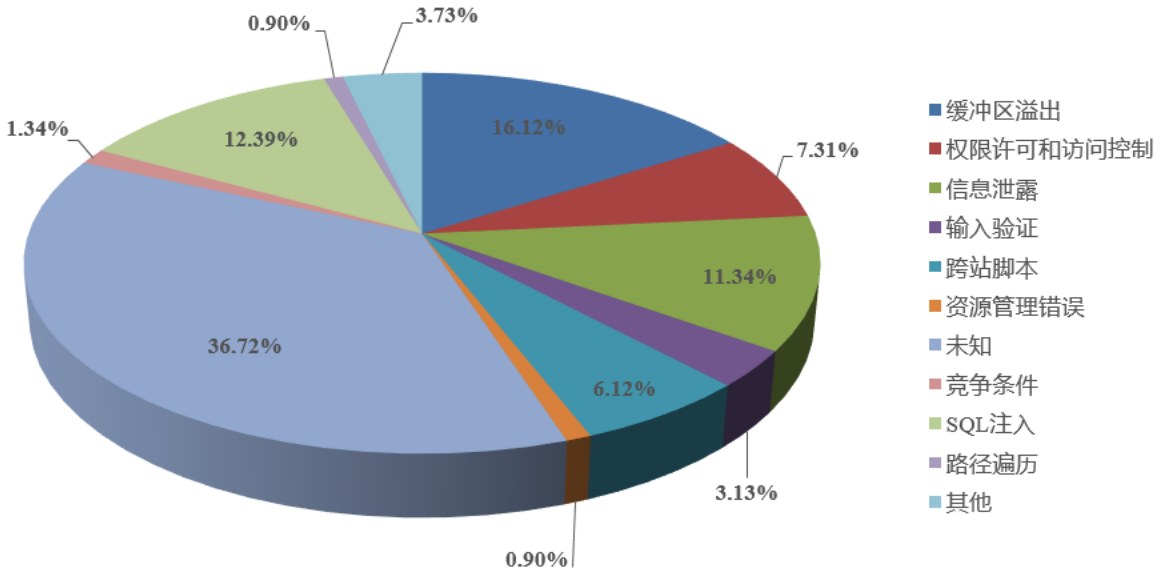

图 1-2 2017 年 12 月漏洞类型占比

三、 高危漏洞实例

(一) Weblogic XMLDecoder 反序列化高危漏洞

CVE 编号：CVE-2017-10271

CNNVD 编号：CNNVD-201710-829

发布时间：2017-12

危险等级：☆☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.1.0

Oracle WebLogic Server 12.2.1.2.0

漏洞描述：Weblogic 是一个基于 Javaee 架构的中间件，用于开发、集成、部署和管理大型分布式 web 应用、网络应用和数据库应用的 Java 应用软件。反序列化漏洞，是指将二进制格式的数据发送给服务器，服务器将其还原成对象代码进行执行，在此过程中存在漏洞，可以执行黑客指定的命令。

近期出现的 Weblogic 反序列化漏洞，被黑客用来获取服务器权限，进行比特币挖矿等黑产活动。该漏洞是利用 WLS 组件的 XMLDecoder 进行攻击，通过精心构造的数据包，可以达到任意代码执行的效果。

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：

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

(二)vBulletin v5 反序列化漏洞

CVE 编号：CVE-2017-17672

CNNVD 编号：CNNVD-201712-488

发布时间：2017-12

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

vBulletin <= 5.3.x

漏洞描述：vBulletin 是一个基于 PHP 和 MySQ 的开源的商业 Web 论坛软件包。

该漏洞与 vB_Library_Template 的‘cacheTemplates()’函数有关，是由于程序没有对用户提供的输入安全的使用‘unserialize()’函数，导致未经验证的攻击者利用该漏洞能够删除任意文件，并且能执行任意恶意代码。

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：目前厂商还未发布升级补丁，及时关注厂商动态：

https://www.vbulletin.com/

(三) OpenSSL 安全漏洞

CVE 编号：CVE-2017-3737

CNNVD 编号：CNNVD-201712-217

发布时间：2017-12

危险等级：☆☆☆☆

漏洞类型：设计缺陷

受影响软件：

OpenSSL 1.0.2b - 1.0.2m

漏洞描述：OpenSSL 是一个强大的安全套接字层密码库，其囊括了目前主流的密码算法，常用的密钥，证书封装管理功能以及 SSL 协议，并提供丰富的应用程序供测试戒其它目的使用。

OpenSSL 从 1.0.2b 版本开始，引入了“error state”机制。如果在握手过程中出现了”fatal error”，那么应用程序会进入”error state”状态，如这时尝试继续握手，应用程序会立即失败。但是如果在”error state”时，SSL_read()或 SSL_write()函数继续被应用程序调用相同的 SSL 对象，由于“error state”处理机制的 BUG，会导致数据可以在没有直接从 SSL/TLS 记录层解密/加密的情况下传递数据。

攻击者利用该漏洞绕过安全机制，执行未授权的操作，危害系统安全。

修补建议：尽快升级到最新稳定版本 1.0.2n。目前厂商已经发布了升级补丁，补丁获取链接：

https://www.openssl.org/news/vulnerabilities.html#toc

(四)Apache Synapse 远程代码执行漏洞

CVE 编号：CVE-2017-15708

CNNVD 编号：CNNVD-201710-1018

发布时间：2017-12

危险等级：☆☆☆

漏洞类型：远程代码执行

受影响软件：

Apache Synapse version < 3.0.1

漏洞描述：Apache Synapse 是 Apache 软件基金会的一款轻量级的企业服务总线。ApacheSynapse 支持 HTTP/S，邮件（POP3，IMAP，SMTP），JMS，TCP，UDP，VFS，SMS，XMPP 和 FIX 。

该漏洞与‘Apache Commons Collections’组件有关，使用了低版本的库 commons-collections-3.2.1.jar。且默认情况下，Java 远程方法调用（RMI）不需要对请求的对象类型进行验证。在 Apache Synapse 启动后就会开启 RMI 服务，攻击者利用该漏洞实现远程代码执行。

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://lists.apache.org/thread.html/77f2accf240d25d91b47033e2f8ebec84ffbc6e6627112b2f98b66c9@%3Cdev.synapse.apache.org%3E

(五)WordPress custom-map 插件跨站脚本漏洞

CVE 编号：CVE-2017-17744

CNNVD 编号：CNNVD-201712-698

发布时间：2017-12

危险等级：☆☆☆

漏洞类型：跨站脚本

受影响软件：

WordPress custom-map <= 1.1

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。

该漏洞与 view/advancedsettings.php 文件的‘map_id’参数有关，未对其进行正确的过滤，远程攻击者可以利用该漏洞进行任意的 Werb 脚本或 HTML 注入。

该漏洞会导致敏感数据泄露，危害系统安全。

修补建议：尽快更新到最新稳定版本，目前厂商已经发布了升级补丁，补丁获取链接：https://wordpress.org/plugins/custom-map/

四、 本月安全要闻

(一)以太坊交易平台 EtherDelta 被黑，失窃近 27 万美元以太币

据外媒 12 月 27 日报道，以太坊交易平台 EtherDelta 的域名服务器（DNS）证实近期遭到黑客攻击，致使 308 以太币（约合$266,789）及潜在价值数十万美元的代币被窃。据悉，此次网络攻击发生于本月 20 日，一度导致 EtherDelta 平台暂停服务，官方当日发表推文公布其 DNS 服务器遭受攻击等相关细节。直至 22 日 EtherDelta 平台才完全恢复服务。

知情人士透露，此次黑客主要通过 DNS 劫持诱骗用户发送钱款。官方指出伪造的应用程序中不仅没有导航栏上的聊天按钮，也没有官方 Twitter 提要，并且还具有一个伪造的订单簿以便获取用户信任。

EtherDelta 在其推文中呼吁所有用户不要访问假冒的网站，并承诺使用 MetaMask 和 hardware 钱包的用户不会受到影响，以及从未在钓鱼网站上输入私钥的用户也是安全的。

目前全球各地已发生多起黑客入侵虚拟货币平台事件，如近期韩国加密货币交易所 Youbit 在今年第二次遭受重大攻击后宣布破产，加密货币矿业市场 NiceHash 也证实因黑客攻击导致价值 6000 万美元的比特币损失。研究人员认为虚拟货币价格的飙升是吸引网络犯罪分子频繁进行攻击行动的主要原因。

友情链接：http://www.safedog.cn/news.html?id=2452

(二)俄罗斯黑客从美俄 ATM 窃取千万美元，下一目标锁定拉美银行

据媒体 12 月 12 日报道，俄罗斯网络安全公司 Group-IB 于 12 月 11 日表示，一个此前未被检测到的俄语黑客组织，在 2016-2017 年间通过瞄准银行转账系统，从至少 18 家银行机构中悄然窃取了近千万美元，这些金融机构大多为美国和俄罗斯的公司组织。该黑客组织发起的攻击始于 18 个月前，他们利用转账系统漏洞从银行的自动柜员机（ATM）中窃取钱财。Group-IB 警告称，目前针对银行的攻击似乎正在进行中，拉丁美洲的银行可能会成为下一个目标。

Group-IB 研究人员在一份长达 36 页的报告中指出，这一黑客组织首次攻击发生在 2016 年春季，针对的是美国最大的银行信息系统——美国银行 First Data 的“STAR”网络，该系统连接了超过 5000 家机构的 ATM 机。

Group-IB 曾将黑客组织称为“赚钱者（MoneyTaker）”。据悉，该黑客组织此前使用过名为“MoneyTaker”软件来劫持支付订单，然后通过一个低级的、名为“金钱骡子（money mules）”网络从自动柜员机中提取资金。

Group-IB 安全研究人员表示，他们已经确定 18 家银行机构受到了攻击，其中包括分布在美国 10 州的 15 家银行金融机构，两家俄罗斯银行以及一家英国银行。除银行外，金融软件公司和一家律师事务所也成为了攻击目标。

Group-IB 称，在美国遭受攻击的 14 个 ATM 机上，每起被盗事件损失的资金平均为 50 万美元。俄罗斯每起事件平均损失为 120 万美元，但其中一家银行成功截获了一起攻击事件，并追回了部分被盗资金。这一黑客组织还窃取了拉丁美洲及美国 200 家银行所使用的 OceanSystems 美联储链接传输系统内的文件。此外，他们还成功地攻击了俄罗斯的银行间通讯系统——AW CRB。

Group-IB 称，一旦黑客侵入了目标银行和金融机构，他们会窃取银行内部文件，为将来发动 ATM 攻击做准备。在俄罗斯，黑客入侵银行系统后会继续对银行网络进行监控，至少有一家美国银行的文件被盗用了两次。Group-IB 表示，其已通知国际刑警组织和欧洲刑警组织，以协助针对该案的执法调查。

这些身份不明的黑客利用不断变化的工具和战术，绕过反病毒和其他传统安全软件，同时又在小心翼翼地清除他们的操作痕迹，从而避开监控。为了掩饰他们的举动，黑客们使用了来自美国银行、美联储、微软和雅虎等品牌的安全证书。

友情链接：http://hackernews.cc/archives/18155

(三)暗网暴露 14 亿明文密码库，或成史上最大规模数据泄露案

据外媒报道 ,美国一家网络情报公司 4iQ 于 12 月 5 日在暗网社区论坛上发现了一个大型汇总数据库，其中包含了 14 亿明文用户名和密码组合，牵涉 LinkedIn，MySpace，Netflix 等多家国际互联网巨头。研究人员表示，这或许是迄今为止在暗网中发现的最大明文数据库集合。

4iQ 研究员称他们在暗网搜寻被窃、泄露数据时从一个超过 41GB 的文件中发现了这个汇总的交互式数据库。该档案最后一次于 11 月 29 日更新，其中汇总了 252 个之前的数据泄露和凭证列表、包含 14 亿个用户名、电子邮件和密码组合、以及部分比特币和狗狗币（Dogecoin）钱包。

据统计，这 14 亿数据由早期泄露的数据和凭证列表汇总而成，密码部分来自 Anti Public，Exploit.in 等凭证列表，多涉及 Anti Public、Exploit.in、LinkedIn、MySpace、Netflix、比特币、Pastebin、FM,Zoosk、YouPorn、Badoo、RedBox 等互联网公司以及类似 Minecraft 和 Runescape 这类游戏公司。

此次发现的数据量几乎是此前最大凭证泄露事件的两倍，光是 Exploit.in 凭证列表就包含 7.97 亿条记录，而最新泄露数据中还增加了 3.85 亿新的凭证组合、3.18 亿用户和 1.47 亿密码。

然而令人担忧的是，这些密码都没有进行加密。研究人员通过随机抽检发现大部分都是真实密码，其中大约有 14%的用户名和密码组合以前并未被黑客社区解密，而现在却以明文形式呈现。由于数据库早已按照字母顺序整齐排列并编入索引，因此任何具备基本网络知识的人都能快速搜索密码 ,例如 ,仅需简单地搜索就能从数据库中找到 226,631 个使用“admin”、“administrator”或者“root”的常见密码。据统计，此批数据库中最常用的密码依旧是“123456”、“123456789”、“qwerty”、“password” 和 “111111”等。

目前尚未知究竟何人将数据库上传至暗网论坛，且不管此人有何目的，显然他们都已将 14 亿用户账号安全置于危险境地。对此研究人员建议，为保护账户安全，互联网用户们谨记在各类在线帐户中设置复杂密码，并且避免多账号使用相同密码。

友情链接：http://hackernews.cc/archives/18191

(四) JulySystems 公司“ProximityMX”平台因 AWSS3 存储器配置不当致敏感数据泄露

据外媒报道，总部位于旧金山的 July Systems 公司在网上暴露了大量敏感数据，该公司基于云智能定位和参与平台“Proximity MX”通过不安全的 Amazon S3 数据库公开了公司及其客户的专有信息。相关安全人员表示，极有可能是因为人为因素而造成了此次暴露事件。

相关人士透露，July Systems 的 Proximity MX 平台连接个人的数字足迹，特别是跟踪消费者的消费行为。该平台允许公司的客户与消费者进行相关的优惠和促销，并将数据记录到系统中。据悉，该平台使用者还包括 CNN，ESPN，Intel，Toys“R”Us，CBS，Fox 和 NB Universal 等全球知名媒体公司。

经过调查，在过去的一年中，配置不当的 S3 存储器造成的多次大规模泄漏事件已经暴露了来自各个组织的大量数据。最近，美国陆军和国家安全局的数据也被暴露。而此次 July Systems 泄露的数据包括 iPhone 和 Android 应用程序的安全凭证，存储库凭据（可能允许任何人访问敏感的客户端数据或跟踪数据），内部构建和各种客户端的开发工具（比如 NFL，CBS，Amex，NBA，FOX，PGA 等）。此外，还暴露了诸如“Katy Perry，NFL，NBA”等品牌的档案信息和印度 Unilever 管理者的 1000 个用户名和密码。

Diachenko 表示，此次暴露事件很可能是人为造成的 。因为 July Systems 有几台 S3 服务器没有密码并且可以公开访问。但目前不清楚是否有其他第三方访问了这些数据库，也不清楚该公司的 S3 存储器在被发现之前还要暴露多久。July Systems 在被告知数据暴露的两天内就已锁定涉事 S3 存储器，但与 Cisco 相关的服务器在获得安全保护之前仍然暴露了一个星期，然而现在真正的考验是，网络犯罪分子可能利用暴露的密码来访问数据基础设施的安全区域。

友情链接：http://storage.cnw.com.cn/eyan/571422.html

(五)逾六千台装备 Lantronix 串口的以太网设备暴露 Telnet 密码，可连接关键工控系统

NewSky Security 的首席安全研究员 Ankit Anubhav 于近期发现数千台装备 Lantronix 串口的以太网设备泄漏了 Telnet 密码。知情人士透露，攻击者可以借此针对连接设备发动网络攻击。

据悉，该设备服务器由美国供应商 Lantronix 制造，并被广泛应用于连接工控系统，其中大部分是老旧设备（只具备串行端口）。调查显示，此次暴露的以太网服务器串口是转用于连接远程设备的接口，例如：产品 UDS 和 xDirect 可以轻松通过 LAN 或 WAN 连接管理设备，从而实现与具备串行接口的任何设备进行以太网连接。

Anubhav 表示，当前逾有 6,464 台可连接到关键工控系统的 Lantronix 设备服务器在线泄露了 Telnet 密码，这些设备在 Shodan 上的曝光占了 48%。据称，此次泄露事件不仅允许攻击者接管设备后使用特权访问将串行命令发送至连接设备，还能够允许攻击者可以通过在端口 30718 上发送一个格式错误的请求检索 Lantronix 设备配置。

另外，研究人员发现在 Metaploit 黑客平台包括一个 Lantronix“Telnet 密码恢复”模块，该模块可用于通过配置端口（旧版本的 Lantronix 设备默认启用 30718/udp）从 Lantronix 串口到以太网设备检索安装设置记录，并以明文方式提取 Telnet 密码。目前，补丁管理再次成为问题根源，而且易受攻击的设备并未（难以）通过更新来解决此类问题。

友情链接：http://www.safedog.cn/news.html?id=2371

