迪普科技 2018 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

2018 年 12 月份新增安全漏洞 1156 个。比上月增加了 165 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 82 个，中危漏洞 206 个，低危漏洞 868 个，同比 2017 年 12 月（漏洞总数 670 个）增加 42.04%。表 1-1 为 2018 年 7 月-2018 年 12 月漏洞危险等级统计。

表 1-1 2018 年 7 月-2018 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	10	80	4	13	2	82
中危	320	661	14	177	9	206
低危	1593	197	1173	1251	980	868
总数	1923	938	1191	1441	991	1156

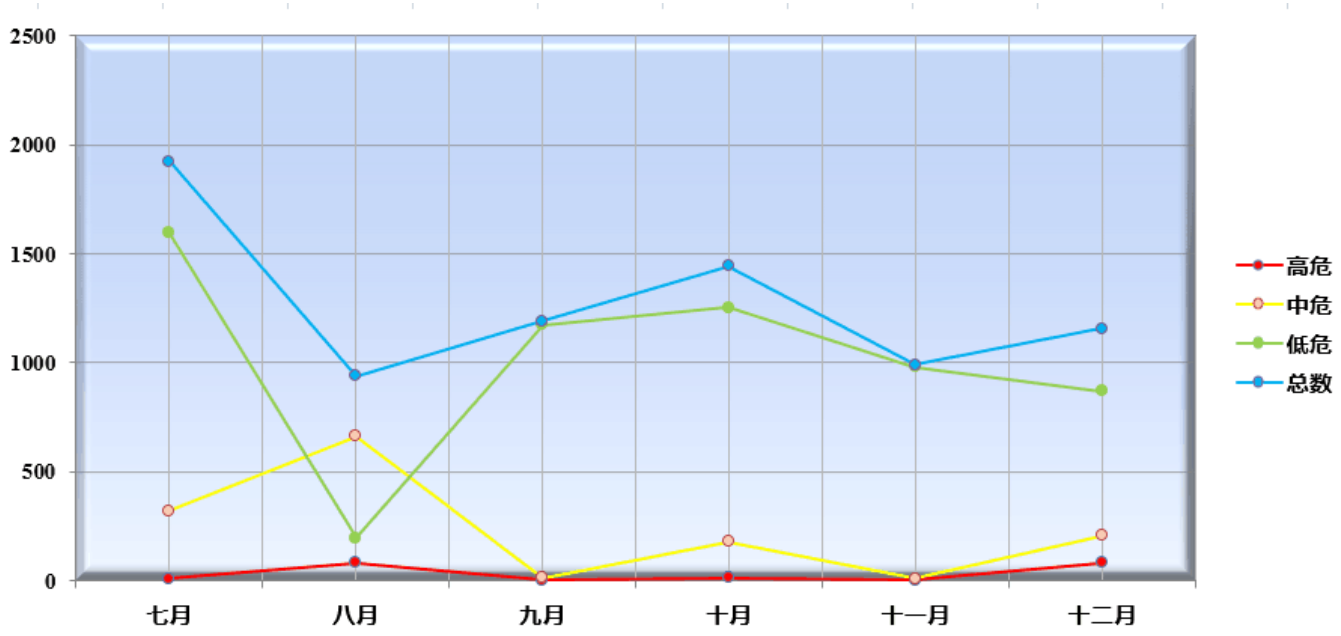

图 1-1 2018 年 7 月-2018 年 12 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 12 月份新增的漏洞类型分布如表 1-2 所示。其中跨站脚本，占 15.74%。值得关注的还有信息泄露、SQL 注入、权限许可和访问控制等常见漏洞类型。

表 1-2 2018 年 12 月漏洞类型分布

类型	数量	比例
未知	685	59.26%
跨站脚本	182	15.74%
跨站请求伪造	23	1.99%
信息泄露	51	4.41%
SQL 注入	31	2.68%
权限许可和访问控制	39	3.37%
路径遍历	21	1.82%
输入验证	27	2.34%
操作系统命令注入	11	0.95%
缓冲区溢出	28	2.42%
其他	191	5.02%

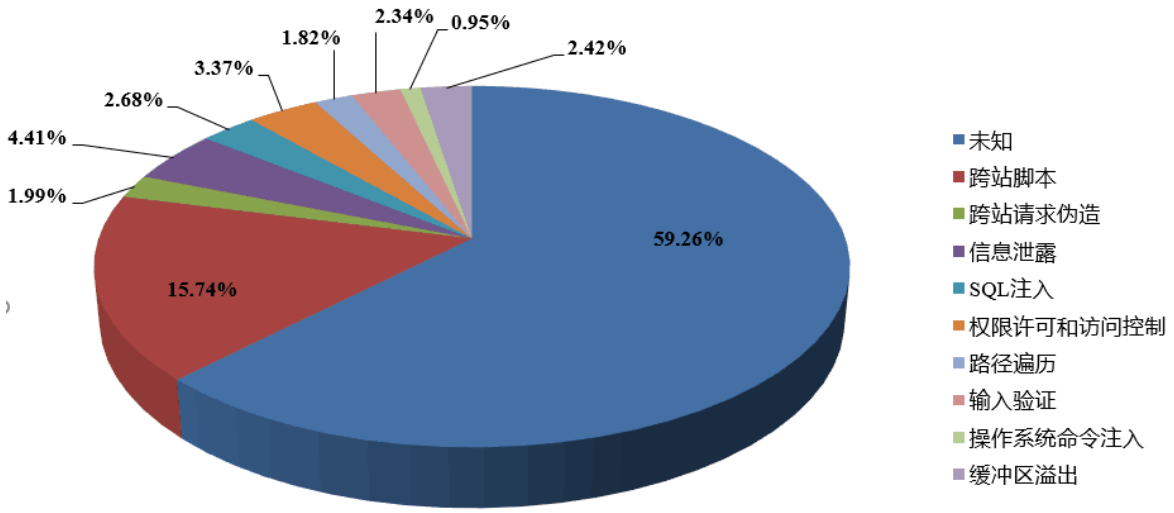

图 1-2 2018 年 12 月漏洞类型占比

三、 高危漏洞实例

（一）Discuz! DiscuzX 安全漏洞

CVE 编号：CVE-2018-20424

CNNVD 编号：CNNVD-201812-1074

发布时间：2018-12

危险等级：☆☆☆

漏洞类型：权限许可和访问控制

受影响软件：

Discuz! DiscuzX 3.4

漏洞描述: Discuz!X 是一个采用 PHP 和 MySQL 等其他多种数据库构建的性能优异、功能全面、安全稳定的社区论坛平台。

该漏洞与受影响版本中 plugin.php 页面有关。在微信登录启用的前提下，通过向受影响页面发送特制的请求可以删除 common_member_wechatmp 数据结构。远程攻击者可以利用该漏洞提升自身权限，从而控制被攻击网站。

攻击者可以利用该漏洞获得管理员权限，危害系统安全。

修补建议：目前厂商已发布补丁，补丁获取链接：

https://gitee.com/ComsenzDiscuz/DiscuzX

（二）PHP 安全漏洞

CVE 编号：CVE-2018-19935

CNNVD 编号：CNNVD-201812-293

发布时间：2018-12

危险等级：☆☆

漏洞类型：数字错误

受影响软件：

PHP 5.x

PHP 7.x < 7.3.0

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。

该漏洞与受影响版本中 ext/imap/php_imap.c 文件存在安全漏洞有关。受影响版本中 imap_mail 函数的 message 参数对输入验证不足。远程攻击者可以利用该漏洞造成拒绝服务攻击，影响网站业务的稳定性。

攻击者可以利用该漏洞发起拒绝服务攻击，危害系统安全。

修补建议：目前厂商已经发布补丁，补丁获取链接：

https://bugs.php.net/bug.php?id=77020

（三）Mini-XML 缓冲区错误漏洞

CVE 编号：CVE-2018-20004

CNNVD 编号：CNNVD-201812-376

发布时间：2018-12

危险等级：☆☆☆

漏洞类型：缓冲区溢出

受影响软件：

Mini-XML 2.12

漏洞描述：Mini-XML (MXML) 是一款使用 C 语言开发的小型 XML 解析器，无需其他类库而只需要 GCC 编译器和 make 程序即可完成编译，且支持 UTF-8 和 UTF-16 编码。

该漏洞是与受影响版本中 mxml-file.c 文件的‘mxml_write_node’函数存在栈缓冲区溢出问题有关，是由牵涉到双精度浮点数和'<order type = “real” >'子字符串的向量引起。攻击者可利用该漏洞执行恶意代码。

攻击者可以利用该漏洞执行恶意代码，危害系统安全。

修补建议：目前厂商已经发布补丁，请向供应商咨询详情。

https://github.com/michaelrsweet/mxml/issues/233

（四）VeryNginx 安全漏洞

CVE 编号：CVE-2018-19991

CNNVD 编号：CNNVD-201812-338

发布时间：2018-12

危险等级：☆☆

漏洞类型：输入验证

受影响软件：

VeryNginx 0.3.3

漏洞描述：VeryNginx (Very powerful and friendly Nginx)是一款逻辑部分基于 Lua_Nginx_Module(openrestry) 开发，前端部分基于 HTML/CSS/JS 开发的 Nginx 扩展程序，实现了更高级的防火墙，访问统计以及 WEB 操作配置等功能。

该漏洞与受影响版本中 get_post_args 和 get_uri_arg 函数对预期参数缺少错误处理有关，远程攻击者可以利用该漏洞提交超过预期数量的参数来规避 WAF(Web 应用防火墙）防护，从而发起网络攻击。

攻击者可以利用该漏洞绕过 Web 应用防火墙防护，危害系统安全。

修补建议：目前厂商还未发布补丁，请向供应商咨询详情。

https://github.com/alexazhou/VeryNginx/issues/218

（五）Wordpress Master Slider Plugin 跨站脚本漏洞

CVE 编号：CVE-2018-20368

CNNVD 编号：CNNVD-201812-1027

发布时间：2018-12

危险等级：☆☆☆

漏洞类型：跨站脚本

受影响软件：

WordPress Master Slider Plugin 3.2.7

WordPress Master Slider Plugin 3.5.1

漏洞描述：WordPress 是一款采用 PHP 语言和 MySQL 数据库开发的个人博客系统，同时也可以当成一款内容管理系统来使用。WordPress Master Slider Plugin 是一款可以给网站添加幻灯片效果的 WordPress 插件，支持在移动设备上触屏操作。

该漏洞与受影响版本中 wp-admin/admin-ajax.php 路径下 Callback 的 MSPanel.Settings 值的 Name 输入字段未进行验证过滤有关，攻击者可利用该漏洞执行恶意的脚本或代码。

攻击者可以利用该漏洞写入任意代码，危害系统安全。

修补建议：目前厂商还未发布补丁，请向供应商咨询详情。

https://wordpress.org/plugins/master-slider/

四、 本月安全要闻

（一）NASA 服务器被黑客攻击，员工信息曝光

美国国家航空航天局（NASA）已确认旗下一台服务器在 10 月被黑客攻击，黑客从其中盗取了一些员工信息，包括社会安全号码等等。在 12 月 18 日发布的通知中，美国国家航空航天局表示，它目前正在通知那些可能因此受到损害的员工。调查已经开始，NASA 表示社会安全号码和其他个人身份信息存储在被黑的服务器上。

NASA 表示，在发现这些事件后，NASA 网络安全人员立即采取行动保护服务器及其中包含的数据。美国宇航局及其联邦网络安全合作伙伴正在继续检查服务器，以确定潜在数据泄漏的范围，并识别可能受影响的个人。NASA 表示，调查需要时间，但强调它现在已成为 NASA 目前最重要的优先事项。

该机构声称没有任何迹象表明 NASA 的各项任务受到了黑客影响，但现在它已经传达给所有员工，让他们知道某些信息已经暴露给黑客。NASA 表示，将为所有员工提供额外服务，包括身份保护服务。

但是 NASA 没有详细说明服务器是如何被破坏的，以及事件背后的黑客组织名称。

友情链接：https://www.cnbeta.com/articles/tech/800189.htm

（二）Gmail 账号 5200 万用户数据泄露，谷歌将提前 4 个月关闭 Google+

北京时间 12 月 11 日早间消息，谷歌周一表示，将于明年 4 月关闭 Google+社交 1.编写日志处理脚本媒体服务，比原计划提前 4 个月。此前，该公司今年第二次发现 Google+的软件漏洞，新漏洞导致合作伙伴应用能访问用户的个人数据。

不过谷歌在博客中表示，没有发现任何证据表明，其他应用使用该必应漏洞访问了这些数据，包括用户的姓名、电子邮件地址、性别和年龄。谷歌表示，在上月引入的 6 天时间内，该漏洞影响了 5250 万个 Google+帐号，其中包括一些企业客户的帐号。

本周，谷歌 CEO 桑达尔·皮猜（Sundar Pichai）将在美国国会众议院司法委员会就谷歌的数据收集行为作证。美国两党议员正呼吁制定新的隐私保护立法，以更好地控制谷歌、Facebook 和其他大型科技公司。

今年 10 月，谷歌表示，将于 2019 年 8 月关闭 Google+的消费级版本，因为维护该服务带来了太大的挑战。当时该公司表示，来自 50 万用户的个人信息数据可能被一个已经存在两年多的漏洞泄露给合作伙伴应用。

谷歌表示，在获得用户授权情况下从 Google+获取数据，用于服务个性化的应用将会在 90 天内失去数据访问权限。与此同时，为企业客户开发 Google+仍将是该公司的一大关注点。

友情链接：https://tech.sina.com.cn/i/2018-12-11/doc-ihmutuec8036940.shtml?cre=tianyi&mod=pctech&loc=16&r=25&doct=0&rfunc=28&tj=none&tr=25

（三）数据泄露——维多利亚州政府雇员详情外泄

据 ABC 1 月 1 日报道，不知名政党下载了部分维多利亚州政府名录后，3 万名维多利亚州公务员工作详情数据遭窃。

这个给政府员工使用的名录包含工作电邮、职称以及工作电话号码。

受此次数据泄露事件影响的员工通过邮件被告知，在通讯录上的员工的电话号码可能也已外泄。

电邮称，“此事件后，你可能会遭受更多来自电邮和电话的网络钓鱼攻击、垃圾电邮及社交工程攻击。”

“通常而言，你应当重视这些风险，并对这些通过电邮及电话号码传播的垃圾通信保持警惕。”

工作人员被告知称，此次数据泄露事件并未影响银行及财务信息。

墨尔本大学网络安全和隐私研究员 Suelette Dreyfus 表示，尽管目前似乎并无非常个人及敏感数据外泄，数据集作为一个整体可能会被用于更有针对性的攻击。

Dreyfus 博士表示，“若将小段数据汇总为数据集，你便可获知整个州政府的形象，因为由此你可了解所有不同的人、其位置、电话号码.....而且，你还可推测出权力中心的位置，以及你应有针对性的入侵何人的电邮。”

她表示，数据集对任何试图影响政府决策的人都很有价值。

她说:“无论是为了赢得一份合同而进行的商业活动，还是因为你是一个可能有利益的国际国有企业——无论是在金融方面还是在政策方面——所有这些类型的人都可以从实际上被黑客窃取的信息中获益。”

总理府表示已将该泄露事件移交警方、澳大利亚网络安全中心和维多利亚州信息专员办公室调查。

该部门的发言人声明道，“为防止再次发生此类数据泄露事件，政府将妥善处理所有调查所得。”

友情链接：https://www.easyaq.com/news/520548145.shtml

（四）中国很安全：全球发现 41.5 万多台路由器受挖矿病毒感染

据外媒报道，日前有研究人员发现，全球有超过 41.5 万台路由器被感染了挖矿病毒，这些路由器中受影响最严重的是 MikroTik 品牌的路由器。

根据记录的数据，目前这一品牌路由器在今年八月份就受到一系列的攻击，当时发现有超过 20 万台设备被感染挖矿病毒。鉴于这一品牌路由器在国内市场非常非常小，中国并没有受到这一挖矿病毒的影响。目前，全球范围内受感染的路由器已经超过了 41.5 万台。主要感染区集中在巴西、欧洲、印度和东南亚。

这些路由器被感染后会秘密的开采加密货币，安全专家建议受到影响的路由器立即升级最新的固件，针对这一恶意病毒的补丁已经发布数月，尽管有不少的用户已经通过升级固件摆脱困扰，但对于全球范围内 41.5 万台的设备来讲，这仍然是杯水车薪。

友情链接：https://www.ithome.com/0/399/346.htm

（五）万豪称 5 亿喜达屋客户信息被泄露，CEO 向公众致歉

11 月 30 日，高端酒店巨头万豪国际集团称下属的喜达屋酒店的大量用户数据可能已经被黑客获得，并且这可能会导致迄今为止最大的用户信息泄漏事件。

万豪酒店通过万豪自身的所有的公众平台对外公布了这一消息，第一时间公开了相关内容细节，并成立了特设网站与电话专线回应公众对此事的问询。

万豪称他们在今年 9 月 8 日收到了一条内部安全检查工具发出的关于第三方试图访问喜达屋宾客预定数据库的警报，在收到该警报后万豪第一时间聘请权威安全专家进行调查。在调查中得知，自 2014 年起就有第三方开始对喜达屋的服务网络进行未授权访问。根据近期第三方的行为，发现他们在复制并加密某些信息，直至昨日，终于解密了信息，确认信息来自于喜达屋宾客预定数据库。

根据万豪的公告，虽然现在未能完成数据的比对，但是万豪认为泄漏数据内为截止至 2018 年 9 月 10 日所有曾在喜达屋酒店预订过的用户信息，包括姓名、电话、身份证件号码、生日、预订信息以及已加密过的部分用户的信用卡号、CVV 码等支付工具信息。虽然已加密数据是通过 AES-128 加密的，但是由于无法确认加密用的公钥与私钥是否有泄漏，故也无法确认该数据是否有泄漏。

万豪国际集团 CEO 苏安厉（Arne Sorenson）在公告内对公众表示“我们对此次事件表示深深的歉意。我们正在积极采取行动，不遗余力的帮助受影响的宾客。”

同时，万豪设立了专门的网站与电话服务中心来处理用户的问询，并通过预留联系方式向所有喜达屋的用户告知此事。

友情链接：http://www.4hou.com/other/14856.html

