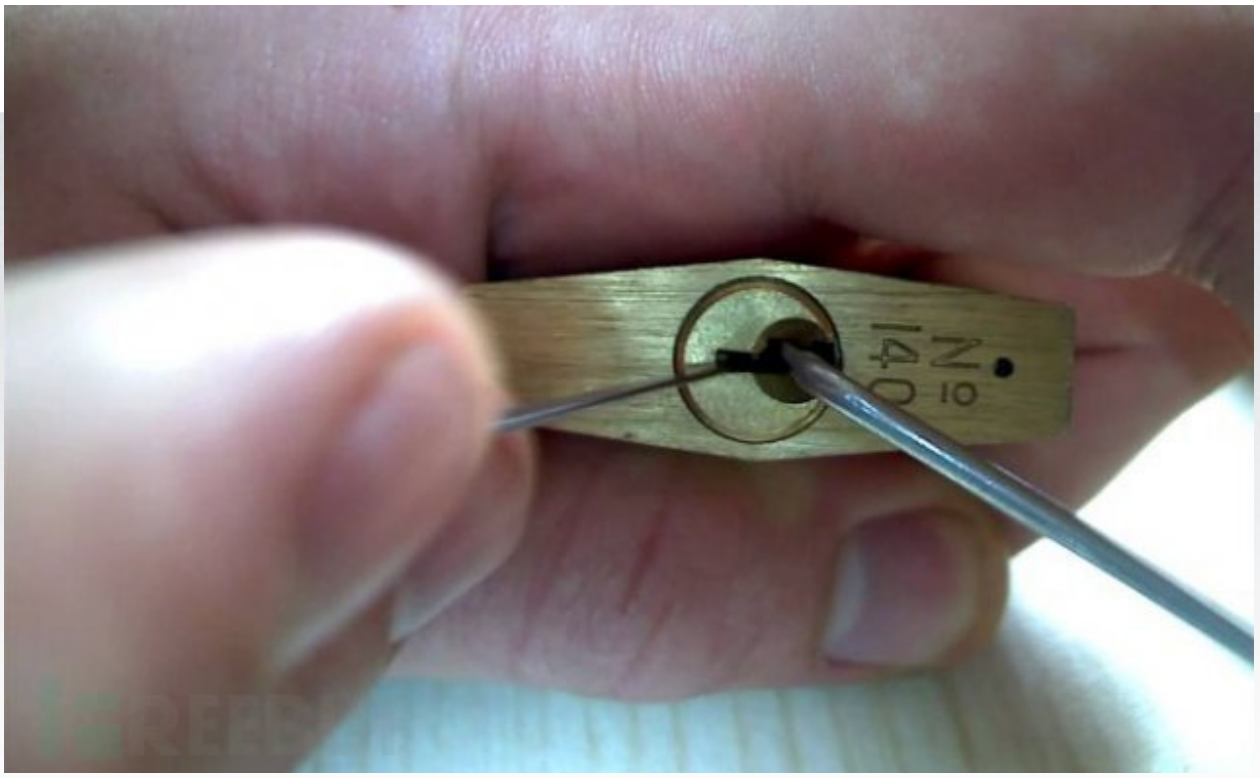

OpenSSL加密代码库的维护者们宣布修复了一个高危漏洞。该漏洞能让黑客获取在HTTPS和其他安全传输层，对加密通信进行解密的密钥。

OpenSSL漏洞细节

当各种条件满足时，该漏洞就可以被利用。首先，这个漏洞存在于OpenSSL v1.0.2。依赖它的应用，必须是使用数字签名算法生成基于DH密钥交换的临时key。默认情况下，该类服务器将复用相同的DH私钥，这会让它更易受到密钥覆盖攻击。基于DSA的DH（Diffie Hellman）配置（依赖于静态DH加密套件），也是会受影响的。

幸运的是，许多主流应用的配置并不是OpenSSL+基于DSA的DH。比如Apache服务器，就开启了SSL_OP_SINGLE_DH_USE选项，这会使用不同的私钥。由OpenSSL衍伸出的BoringSSL 代码库，在几月前抛弃了对SSL_OP_SINGLE_DH_USE支持。而LibreSSL在本周早些时候也已经将这个选项弃用。然而，使用静态加密套件时，这些应用和库仍然是存在漏洞的。

当其他附加条件满足后，黑客可以发送大量的握手请求包到存在漏洞的服务器或者PC机。进行了足够的计算后，黑客会获得部分密钥值，最后结合中国剩余定理，能够推导出完整的解密密钥。这个漏洞编号为CVE-2016-0701，Adobe系统研究员Antonio Sanso于周三发布了一篇博文，里面讲了相关的内容和报告给官方的细节。除此之外，OpenSSL官方警告，这次的解决方案可能会影响机器性能。

OpenSSL修复该漏洞的速度让人惊讶，Sanso是1月12日向官方报告的该漏洞，这意味着官方修复、分发只用了2个多星期。有趣的是，当研究人员报告了漏洞后，解决DH密钥复用的修复进行了更新。但官方现在还没有发布新版本，他们通过补丁完成了部分修复。

还记得Logjam么

周四的发布中还包括了针对一个 HTTPS-crippling漏洞的解决方案，这个叫Logjam的漏洞于去年五月首次披露，影响成千上万的服务器。它允许黑客降级DH加密连接，使用更加脆弱的512位密钥。在这里，

黑客可以使用预先计算好的数据，推断出通信双方的密钥。

如果使用了DH参数，OpenSSL会拒绝少于1024位的密钥通信，此前一个OpenSSL补丁已经增加了768位的限制。

注意，使用OpenSSL v1.0.2的应该升级到1.0.2f，而使用版本1.0.1的应该安装1.0.1r。周四的OpenSSL公告提醒用户，他们对1.0.1的支持将在今年年底结束，后续不会再有安全补丁。而对0.9.8和1.0.0的支持已于12月结束。

***参考来源：AC，FB小编dawner编译，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**