Windows 10中的DPAPI安全漏洞

Passcape Software

1 Windows 10中的DPAPI安全漏洞

1.1 简要说明

我们的专家在DPAPI安全方面发现了一个新的严重漏洞，允许任何人解密Windows 10中最后一个活跃用户的个人数据（由DPAPI保护）。

1.2 哪些操作系统会受到影响？

This vulnerability affects Windows 10, starting with 1709 Fall Creators Update, as well as Microsoft accounts in previous versions of Windows 10 so far the system volume encryption is activated.

1.3 什么是DPAPI？

数据保护应用编程接口（DPAPI）旨在对用户的个人数据、加密密钥、系统关键数据以及其他敏感信息进行安全加密。它是自Windows 2000以来所有Windows操作系统中的一个主要保护子系统。DPAPI之所以受欢迎，主要是因为它很容易使用，因为它只包括两个函数来加密或解密敏感数据。CryptProtectData和CryptUnprotectData。这可能听起来很简单，但CryptProtectData/CryptUnprotectData的内部逻辑相当复杂。你可以在 这篇.中章阅读更多关于DPAPI的工作原理

1.4 以前的DPAPI漏洞

DPAPI的创建考虑到了许多方面的安全性，可以肯定地认为是最好的数据保护系统之一，这是一个设计良好的产品可以服务多年的很好的示例。然而，第一次实施遇到了严重的问题。问题是由于DPAPI v1中的主加密密钥基于用户密码的NTLM哈希。这意味着只需访问NTLM哈希（存储在SAM注册表中）即可解密DPAPI保护的所有密码和数据。幸运的是，微软很快发现了逻辑上的缺陷，并迅速推出了第二个DPAPI修订版，到目前为止，该版本已经正确运行。

新漏洞与第一个问题类似，但以下各项除外：

- 新的DPAPI问题仅影响系统的最后一个活动用户
- 它不适用于域帐户
- 与第一个实现不同，新的漏洞不是开发人员的错误，而是安全性和可用性的被迫妥协。

1.5 什么是自动重启登录(ARSO)？

从Windows 8开始，就开始 启动锁屏应用程序. 也就是说，在用户的会话被锁定时启动、工作和显示通知的应用程序。例如，日历预约、通知、电子邮件、信息等。然而，在升级后的自动重启期间，这些应用程序将停止工作，因为它们需要一个活跃的用户会话。有一个明显的安全冲突，微软已经用一种相当原始的方式解决了这个问题。

就在系统启动自动重启之前，当前的用户凭证被存储在一个特殊的LSA秘密中。重启后，这些凭证被用来自动登录用户并创建一个活动会话，但在用户输入密码、PIN码等之前，互动部分将无法使用。因此，用户的最后一个会话将被自动恢复，锁屏应用程序将发挥作用。这就是自动重启登录系统的简要工作原理。

1.6 什么是受信任的启动自动登录(TBAL)？

在Windows 10中，ARSO使用可信的启动自动登录(TBAL)机制。 自动登录 是Windows的一个内置功能，允许自动登录用户，而不是等待他们输入姓名和密码。自动登录是通过注册表激活的，你需要在注册表中输入用户的明文密码。在启动过程中，系统会检查该选项，如果设置了，就会读取明文密码并使用它来执行登录。

在Windows 10中，自动登录被扩展为TBAL机制。TBAL是一种常见的自动登录和ARSO功能的共生体。但它也有一些不同之处:

- TBAL同时支持普通账户和微软账户
- TBAL不存储明文密码
- TBAL似乎一直处于开启状态，而不仅仅是根据要求。虽然在Windows 10的第一个版本中，系统只在启用全盘加密后才激活TBAL。

那么，TBAL是如何工作的？

1.7 TBAL是如何工作的？

在关闭之前，LSA进程将一个特殊的文本值_TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9}保存到LSA秘密DefaulPassword中，这表明这不是一个普通的自动密码，而是一个TBAL标记。然后，根据活动用户账户的类型，创建另一个LSA秘密。如果这是一个离线账户，系统会将用户名、NTLM、SHA1密码哈希值以及其他一些私人信息存储到名为M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA的LSA秘密。如果这是一个微软账户，那么将创建M$_CLOUDAP_TBAL_{8283D8D4-55B6-466F-B7D7-17A1352D9CAB}_<UID>(Windows 1607及以前)或M$_CLOUDAP_TBAL_{4416F0BD-3A59-4590-9579-DA6E08AF19B3}_<UID>(Windows 1703及以后)秘密，其中<UID>是唯一用户ID的SHA256杂凑。与离线账户的秘密不同，这个秘密只包含推导DPAPI主密钥所需的96字节加密密钥。

在PC重新启动后，系统识别TBAL令牌并使用用户的SHA1哈希值(对于离线账户)或96字节的密钥(如果是微软账户)解密DPAPI主密钥。然后，LSA令牌和LSA密钥的秘密都被删除。

如果系统正在休眠或注销用户，则不会写入TBAL令牌，但仅在重新启动或关机时写入。

1.8 问题的起因是什么？

用户的问题是，在系统关闭后，任何对PC具有物理访问权限的人都可以使用存储的TBAL机密解密DPAPI主键，从而解密使用DPAPI加密的所有用户数据。很明显，该漏洞的原因不是行为不当的逻辑，而是Microsoft对Windows安全的概念性方法。这与第一个DPAPI实现中的方法不同，也与以前的 无密码登录实现中的错误不同.

然而，这似乎是近年来的全球趋势。

1.9 哪些数据有风险？

- 由流行的互联网浏览器保存的网络密码。谷歌浏览器、Internet Explorer、Microsoft Edge、Opera等。
- 电子邮件客户端的密码。Microsoft Office Outlook、Windows Mail。
- 共享文件夹和资源的密码
- 储存在 Windows Vault 中的密码、密钥和其他私人数据
- 远程桌面的密码
- EFS私人密钥，从而访问EFS加密的文件
- S-MIME邮件中的加密密钥
- 用户的证书
- 存储在 Credential Manager 中的网络密码
- 任何应用程序中使用CryptProtectData API保护的任何个人数据，如Skype、Windows权利管理服务、Windows Media、MSN信使、Google Talk等。

1.10 验证

这个视频 展示了在Windows 10中，在不知道他/她的登录密码的情况下，访问最后一个活跃用户的个人数据是多么容易。尽管假设没有人能够在不知道主人的登录密码的情况下做到这一点，但该程序使用TBAL秘密来解密存储在Windows Vault并受DPAPI保护的Facebook凭证。

1.11 总结

正如我们在之前的文章中所警告的那样， 下一个版本的Windows将越来越不注重确保终端用户的安全。对于那些必须提供最大程度保护的用户，建议在Windows 10到1709版本中设置一个离线账户，并设置SYSKEY启动密码或全盘加密。