MicrosoftExchangeSSRF 任意用户伪造(CVE-2018-8581)

安全威胁通告

综述

MicrosoftExchangeServer 中存在一个特权提升漏洞。成功利用此漏洞的攻击者可能会尝试模仿 Exchange 服务器的任何其他用户。要利用此漏洞，攻击者需要执行中间人攻击才能将身份验证请求转发到 MicrosoftExchangeServer，从而允许模拟其他 Exchange 用户。这一漏洞之所以存在，是因为 ExchangeServer 使用 CredentialCache.DefaultCredentials 进行连接。

相关链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8581

https://securitytracker.com/id/1042141

漏洞利用评估

在较旧版本时利用可能较小。在其他版本中，MicrosoftExchangeServer 在受影响版本内，且开启了 ExchangeWebService(EWS)。攻击者需要拥有 MicrosoftExchange 邮

箱账户，Exchange 允许任何用户把订阅推送到指定的 URL，服务器将向此 URL 发送通知。

受影响的版本

MicrosoftExchangeServer2010

MicrosoftExchangeServer2013

MicrosoftExchangeServer2016

MicrosoftExchangeServer2019

检测方法

- 检查 MicrosoftExchangeServer 版本是否为受影响版本。

  MicrosoftExchangeServer2010

  MicrosoftExchangeServer2013

  MicrosoftExchangeServer2016

  MicrosoftExchangeServer2019

- 检查是否开启了 ExchangeWebService(EWS)。

- 相关参考链接：

  https://www.zerodayinitiative.com/blog/2018/12/19/an-insincere-form-of-flattery-impersonating-users-on-microsoft-exchange

解决方案

Microsoft 官方已经发布了对应版本建议,用户应及时进行防护。详情可参考：

临时解决方案：微软建议的临时处置措施：(删除注册表键值)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 是注册表中的注册表项。如果删除此注册表项，CVE-2018-8581 描述的漏洞将无法使用。

打开 CMD 窗口，在 CMD 窗口中输入以下命令。

regdeleteHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa/vDisableLoopbackCheck/f

删除注册表键值后不需要重新启动系统或 ExchangeServer。而且微软强调将来 ExchangeServer 的更新在默认情况下将不再启用该注册表项：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa