MacOS - Privacy hint / OCSP patch

Introduction

The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*.

Wikipedia OCSP Protocol

The OCSP protocol is used to check whether or not a certificate has been revoked. In this context, it is used to give Apple the opportunity to revoke the “blessing” it has given to a specific piece of software. Whenever you start an application, MacOS checks back with the OCSP server.

Resolution

There are two ways to prevent MacOS from checking back to Apple.

Local patch

```
echo 0.0.0.0 ocsp.apple.com | sudo tee -a /etc/hosts
```

Router patch

Discussion

In fact, Apple does not associate the information coming with this request to any person or any IP address. Apple does also not track, when you start an application. Apple could figure out, which software vendor an application is coming from (thinking about Microsoft, that leaves a lot of possibilities).

In the end, it is a simple check whether a certificate is valid or not.

Security professional criticized that a man in the middle attack is possible and you might start an application of which the certificate is revoked. The data itself is also transferred over HTTP without encryption. So a 3rd party could get an idea than somebody runs software from a specific software vendor.

Keeping aside the security concerns, it could be a little bit slower to start an application with a low bandwidth internet connection. In that case, it could make sense to block the request.

Useful links

https://www.sentinelone.com/blog/what-happened-to-my-mac-apples-ocsp-apocalypse/

https://www.theverge.com/2020/11/16/21569316/apple-mac-ocsp-server-developer-id-authentication-privacy-concerns-encryption-promises-fix

---

Revision #1
Created 22 December 2023 09:05:56 by Admin
Updated 22 January 2024 17:34:56 by Admin