2017 年 3 月 27 日，星期一

漏洞聚焦：Apple MacOS 和 iOS 中发现证书验证缺陷，并已得到修复

大多数人在连接银行网站或登录邮件帐户时不会过多地考虑可能会发生什么。在大多数人看来，安全地连接到网站无非就是检查一下地址栏，确保上面显示有小挂锁图标这样简单。但实际上，系统需要在后台执行许多不同的步骤，才能确保您安全可靠地连接到与其显示的名称相符的网站。证书验证便是这些步骤之一，该步骤旨在确保用户尝试连接的服务器能够出示表明其合法身份的“证明”。这有助于保护用户免于登录到可能会窃取敏感信息的欺诈性服务器。

由于这个步骤事关重大，因此如果软件中存在影响证书安全性验证的不良漏洞，则可能会产生严重后果。遗憾的是，全数字化系统非常复杂，而且软件开发过程中难免会出现漏洞。通过发现这些漏洞并本着负责任的态度予以披露，有助于消除潜在的攻击媒介，进而提高互联网安全性。Talos 团队一直致力于提高互联网的整体安全性。本着这样的精神，我们特此披露 Apple MacOS 和 iOS X.509 证书验证功能中存在的远程代码执行漏洞 - TALOS-2017-0296 (CVE-2017-2485)。我们已认真负责地将此漏洞的情况告知 Apple，并针对 MacOS 和 iOS 发布了相应的软件更新以解决此问题。

漏洞详细信息

TALOS-2017-0296 (CVE-2017-2485) 漏洞的发现者是被 Talos 的 Aleksandar Nikolic 发现的。

这个在 Apple MacOS 和 iOS 的 X.509 证书验证功能中发现的释放后再利用漏洞可能会导致攻击者执行任意代码。此漏洞是由于对 X.509v3 证书扩展字段处理不当造成的。攻击者可以使用经特殊设计的 X.509 证书触发此漏洞，导致在受影响的系统上执行远程代码。

在 Apple MacOS 和 iOS 中，大多数客户端应用（例如 Safari、Mail.app、Google Chrome）都使用内置的系统证书验证代理来验证 X.509 证书。如果某个应用将恶意证书传递给证书验证代理，就有可能触发此漏洞。利用此漏洞的攻击场景可能包括：用户连接到向客户端提供恶意证书的网站；Mail.app 连接到提供恶意证书的邮件服务器；或者用户在打开恶意证书文件后将其导入到密钥链。

有关详细信息，请参阅我们的漏洞报告。

Talos 已确认此漏洞存在于 MacOS Sierra 10.12.3 和 iOS 10.2.1 中。更早版本的 MacOS 和 iOS 也可能会受到影响，但是 Talos 尚未确认具体的版本号。

防护

Talos 已开发以下 Snort 规则以检测试图利用此漏洞的攻击尝试。请注意，随着我们获得更多信息，这些规则会相应更新。如需获取最新信息，请访问您的 FireSIGHT 管理中心或 Snort.org。

Snort 规则：41999

保护客户

在软件开发中，不可避免地会出现漏洞。随着全数字化系统日趋复杂，发现可能导致安全问题的漏洞仍将是 Talos 需要持续关注的主要挑战之一。通过研究发现漏洞的方法并认真负责地披露漏洞，我们可以帮助提高客户网络和整个互联网的安全性。

如需了解 Talos 披露的其他漏洞，请访问我们的漏洞报告门户：
http://www.talosintelligence.com/vulnerability-reports/

如需查看我们的漏洞披露政策，请访问以下链接：
http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html

发布者：ALEXANDER CHIU；发布时间：16:09
标签：APPLE、IOS、MACOS、OS X、SNORT 规则、漏洞研究