2017 年 2 月 14 日 星期二

漏洞聚焦：Apple GarageBand 越界写入漏洞

漏洞发现者：思科 Talos 团队的 Tyler Bohan

概述

Talos 披露了 Apple GarageBand 中的越界写入漏洞，TALOS-2016-0262 (CVE-2017-2372) 和 TALOS-2017-0275 (CVE-2017-2374)。GarageBand 是一款音乐创作程序，可供用户在 Mac 电脑上轻松高效地创作和编辑音乐。默认情况下，所有 Mac 电脑均安装了 GarageBand，因此此漏洞的潜在受害者数量非常庞大。在 2017 年 1 月 18 日发布的 CVE-2017-2372 补丁解决了部分问题，随后在 2017 年 2 月 13 日发布的 CVE-2017-2374 补丁彻底解决了此问题。

此特定漏洞是由该应用程序解析 GarageBand 文件使用的专有文件格式 (.band) 的方式所导致的。此格式被分解为多个数据块，每个数据块具有特定长度的字段。此字段长度由用户控制，攻击者可利用它发现可被利用的情况。当用户打开经特殊设计的 .band 文件时，攻击者便可利用此漏洞。有关此漏洞的完整详细信息，请点击此处和此处。

防护

以下 Snort 规则将会检测出漏洞攻击尝试。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

Snort 规则：41350-41351

发布者：WILLIAM LARGENT；发布时间：14:31
标签：零日、APPLE、GARAGEBAND、漏洞、漏洞研究、漏洞聚焦