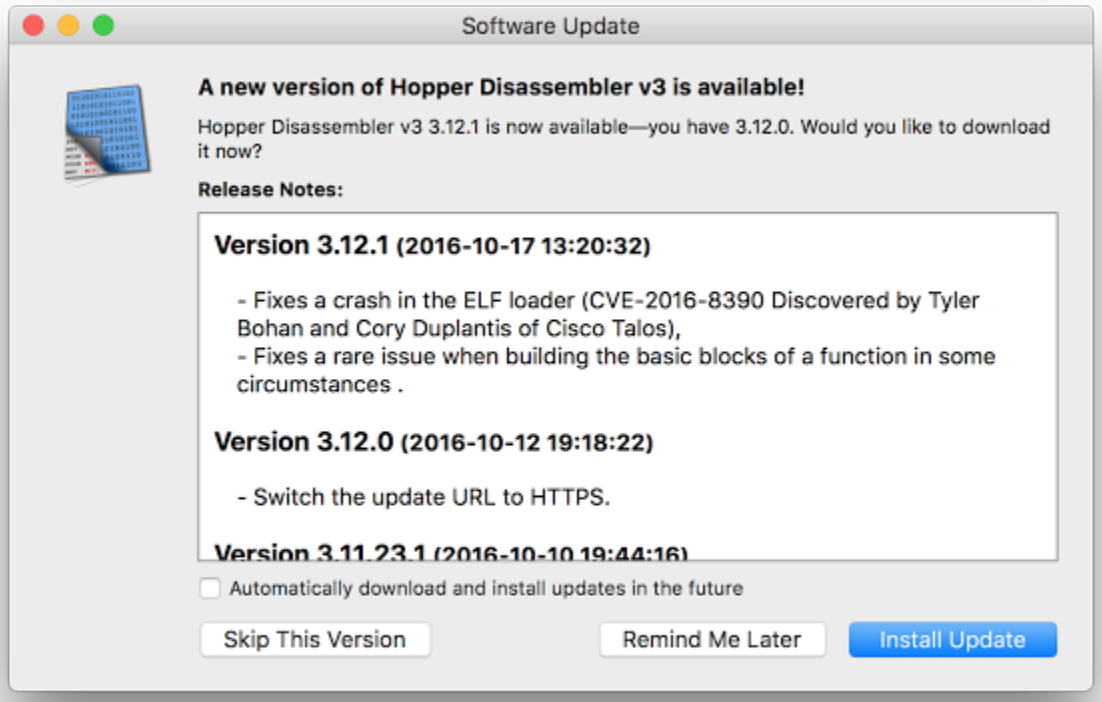
2016 年 10 月 18 日，星期二

漏洞聚焦：Hopper Disassembler ELF 节标头大小代码执行漏洞

漏洞发现者：思科 Talos 团队的 Tyler Bohan 和 Cory Duplantis

Talos 发现 Hopper 的 ELF 节标头解析功能中存在可被利用的越界写入漏洞 (TALOS-2016-0222/CVE-2016-8390)。Hopper 是适用于 macOS 和 Linux 的反向工程工具。利用这个工具，用户可以反汇编和反编译基于 32/64 位 Intel 的 Mac、Linux、Windows 和 iOS 可执行文件。该工具解析 ELF 节标头的过程存在一个未验证且由用户控制的大小值。恶意攻击者可以通过制作包含特定节标头的 ELF 文件触发此漏洞，从而引发远程代码执行。恶意攻击者可以将精心设计的可执行文件压缩到 zip 文件中，并通过网络钓鱼或文件共享网站发送该 zip 文件，以攻击用户。另外，攻击者可以利用这类漏洞逃避分析手段，躲过沙盒分析和自动反汇编。

Hopper 已针对此漏洞做出更新，更改日志可参阅：
https://www.hopperapp.com/rss/html_changelog_v3.php



防护

为了保护我们的客户，Talos 已经发布了相关规则来检测利用该漏洞的攻击尝试。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：40488-40489
http://talosintel.com/vulnerability-reports/
发布者：WILLIAM LARGENT；发布时间：15:26
标签：零日、HOPPER、TALOS、漏洞研究、漏洞聚焦