2016 年 4 月 7 日，星期四

新闻快讯！又一项被利用的 ADOBE FLASH 零日漏洞

就当前威胁形势而言，不幸的 Adobe Flash Player 一直是广受攻击者喜爱的攻击媒介，网络攻击者总是利用它来发动系统攻击。过去的一年里，Talos 发现多起网络攻击者发现并利用 Adobe Flash 零日漏洞攻击系统的案例。据 Talos 的报告显示，Adobe Flash 零日漏洞 CVE-2016-1019 目前正在被攻击者用于攻击 Windows 10 及更早版本的系统。

依据 4 月 5 日发布的 Adobe Flash Player 安全通报，Flash Player 版本 21.0.0.197 及更早版本很容易因 CVE-2016-1019 遭到攻击。受影响的版本包括 Flash Player 版本 20.0.0.306 以及 Flash Player 长期支持版本 (ESR) 18.0.0.333 和更早版本。需要特别说明的是，Adobe 自 2016 年 3 月 10 日起引入了一项缓解措施，防止攻击者利用 CVE-2016-1019 攻击 Flash 版本 21.0.0.182 及更高版本。

鉴于网络攻击者不断利用 Adobe Flash 发起漏洞攻击这一事实，Talos 建议人们采取预防措施来缓解此漏洞的影响，并禁用或删除不必要的浏览器插件。如果无法采取这些措施，Talos 建议所有用户立即升级计算机中的 Flash 软件。对正在使用 Flash Player ESR 的组织而言，这样做尤为重要。依据 Adobe 的通报，21.0.0.182 中引入的缓解措施在 ESR 18.0 版本中未提供。如果用户无法更新或删除 Flash，Talos 建议在浏览器中将 Adobe Flash 设置为“点击播放”形式，或者使用能有效地对 Flash 执行沙盒测试的浏览器。

Talos 将发布以下 Snort 规则来应对这项零日漏洞。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：38429-38434

产品	保护
AMP	✔
CWS	✔
ESA	✔
网络安全	✔
WSA	✔

通过使用 Nuclear 和 Magnitude 漏洞攻击包进行测试，AMP 能够自动防御使用该 Flash 漏洞发起的攻击。

发布者：ALEXANDER CHIU；发布时间：下午 4:24

标签：零日、ADOBE FLASH、AMP、补丁、SNORT 规则、漏洞