2016 年 8 月 10 日，星期三

漏洞聚焦：MS Edge/Windows PDF 库中发现任意代码执行漏洞并已修复

漏洞发现者：思科 Talos 团队的 Aleksandar Nikolic。

昨天，微软针对当前支持的产品中存在的漏洞发布了月度安全公告和补丁集。在昨天发布的公告中，有两个公告被列为“严重”等级，解决了 Microsoft Edge 和 Windows PDF 库中的一个任意代码执行漏洞 CVE-2016-3319。在 Microsoft 发布公告后，Talos 在自己的漏洞报告门户上披露了我们在自己的研究中发现的有关此漏洞的详细信息。

CVE-2016-3319 (TALOS-2016-0170)

CVE-2016-3319 是 Microsoft Edge 和 Windows PDF 库中存在的任意代码执行漏洞。如果用户在存在漏洞的系统中打开经特殊设计的 PDF 文件，则可能会导致系统执行攻击者设置的任意代码。在将 Microsoft Edge 配置为默认浏览器的 Windows 10 系统中，只要浏览托管恶意 PDF 的网站，就会触发此漏洞，因为 Edge 会尝试自动渲染文件内容。需要注意的是，受此漏洞影响的产品包括 Windows 8.1、Windows Server 2012（和 R2）以及 Windows 10。

目前，已有相应的解决方法，可以帮助已安装 Windows 10 且默认浏览器为 Edge 的 PC 降低威胁风险。该解决方法的详细信息可参考 Microsoft 公告 MS16-096 和 MS16-102。

完整的漏洞报告可在以下位置获取：
http://www.talosintelligence.com/reports/TALOS-2016-0170/

Talos 将一如既往地开展研究，努力找出软件中的零日漏洞。通过开发编程方法识别零日漏洞，并本着负责任的态度解决这些漏洞，对于提高互联网整体安全性至关重要。通过我们的研究，我们可以获得有价值的见解，了解如何改进自己的开发实践以及如何帮助修复可能会遭到攻击者利用的软件漏洞（例如 Edge 和 Windows PDF 库中的漏洞）。

以下 Snort 规则可检测此漏洞的攻击活动。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：25459-25460

发布者：Alexander Chiu；发布时间：13:46
标签：Edge、Microsoft、星期二补丁、PDF、漏洞、漏洞研究