2016 年 7 月 8 日，星期五

漏洞聚焦：Symantec Norton Security IDSvix86 PE 远程系统拒绝服务漏洞

漏洞发现者：思科 Talos 团队的 Piotr Bania

Talos 发现 Symantec Norton Security 的可移植可执行 (PE) 文件扫描功能存在拒绝服务漏洞 (CVE-2016-5308/TALOS-2016-0182)。利用经特殊设计的 PE 文件，攻击者可以在 IDSvix86 解析 PE 文件时在其内核驱动程序中造成访问冲突，从而导致拒绝服务。

利用此漏洞的恶意攻击者可能会通过在节头使用较大的 SizeOfRawData 字段来制作特殊设计的文件，然后使用电子邮件将该文件发送给受害者。由于解析器不会执行检查来确保字段大小不会超出文件的限制，也不会对可能导致分段错误的 MD5Compress 功能执行检查，所以在参数足够大的情况下，就会导致 MD5Compress 功能访问当前不可用的内存，从而导致计算机宕机。

Talos 通过与 Symantec 协作，本着负责任的态度披露这一漏洞。发现新的零日漏洞不仅有助于整体提高客户所用软件的安全水平，而且使我们能够直接改善自身安全开发生命周期的各个程序，进而提高所有思科产品的安全性。

此漏洞可通过 SID 39466 和 39467 进行检测。

有关最新的 SID 列表，请访问 FireSIGHT 管理中心防御中心。如需获取更多有关零日攻击或漏洞的报告和信息，请访问：
http://talosintel.com/vulnerability-reports/

有关完整的漏洞公告，请参阅：TALOS-2016-0182。

发布者：William Largent；发布时间：上午 10:07
标签：零日、安全、Talos、漏洞聚焦