2017 年 6 月 30 日，星期五

漏洞聚焦：Dell Precision Optimizer 和 Invincea 漏洞

漏洞发现者：思科 Talos 团队的“冰壁”Marcin Noga。

概述

Talos 针对 Dell Precision Optimizer 应用服务软件、Invincea-X 和 Invincea Dell Protected Workspace 中存在的漏洞发布了公告。这些软件包预装在某些 Dell 系统上。攻击者可以利用这些应用中存在的漏洞禁用安全机制，提升权限，并在应用用户的环境中执行任意代码。

漏洞详细信息

权限提升漏洞 TALOS-2016-0256 (CVE-2016-9038)

此漏洞是 SboxDrv.sys 驱动程序中存在的 Double Fetch 漏洞。攻击者将经特殊设计的数据发送到所有人都可以读取/写入的 \Device\SandboxDriverApi 设备驱动程序，就可以触发此漏洞。一旦攻击者成功利用了此漏洞，即可将任意值写入内核内存空间，进而提升本地权限。

已知存在漏洞的应用：Invincea-X、Dell Protected Workspace 6.1.3-24058

有关更多详细信息，请查看漏洞报告：TALOS-2016-0256。

绕过安全保护漏洞 TALOS-2016-0246 (CVE-2016-8732)

Invincea Dell Protected Workspace 是 Dell 提供的安全解决方案，旨在为终端提供增强的安全保护。其中一个驱动程序组件“InvProtectDrv.sys”（包含在此软件的 5.1.1-22303 版本中）内存在多个安全漏洞。由于对驱动程序通信通道的限制比较薄弱，再加上验证不充分，在受感染系统上执行的攻击者控制的应用，能够利用该驱动程序有效禁用软件提供的某些保护机制。

已知存在漏洞的应用：Invincea、Dell Protected Workspace 5.1.1-22303
此漏洞已在软件的 6.3.0 版本中修复。
有关更多详细信息，请查看漏洞报告：TALOS-2016-2046。

绕过安全保护漏洞 TALOS-2016-0247 (CVE-2017-2802)

在 Dell Precision Optimizer 应用提供的“Dell PPO Service”启动期间，程序“c:\Program Files\Dell\PPO\poaService.exe”会加载 dll“c:\Program Files\Dell\PPO\ati.dll”，进而导致尝试加载“atiadlxx.dll”（默认情况下不会出现在该应用的目录中）。此程序会在 PATH 环境变量指定的目录中搜索具有相应名称的 dll。如果找到同名 dll，它会将该 dll 加载到 poaService.exe 中，而不检查该 dll 的签名。这样一来，如果攻击者提供了具有正确名称的恶意 dll，就可能导致执行任意代码。

Dell 已发布解决此问题的更新。V4.0 以上的所有版本不会受到此漏洞攻击，有关详细信息，请访问：www.dell.com/optimizer。

已知存在漏洞的设备：配备 Nvidia 显卡、PPO Policy Processing Engine (3.5.5.0)、ati.dll（PPR 监控插件）(3.5.5.0) 的 Dell Precision Tower 5810。

有关更多详细信息，请查看漏洞报告：TALOS-2016-2047。

安全影响

鉴于 Invincea Dell Protected Workspace 应用通常部署在高安全性环境中的安全工作站上，我们建议，如果组织使用的是此解决方案的受影响版本，应尽快更新到最新版本，以便确保攻击者无法绕过此软件提供的安全保护。组织需要仔细地综合考虑与设备捆绑的软件带来的风险和优势。任何软件都可能包含可被利用的漏洞。捆绑软件可以提供有用的功能，但如果功能没有得到使用，它会长期保留在设备上，使组织面临漏洞风险，而根本不会提供任何优势。与处理任何未使用的软件一样，删除软件即可删除相关漏洞并从修补计划中删除额外的数据包。

防护

以下 Snort 规则可检测试图利用这些漏洞的行为。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所有信息，请参阅 FireSIGHT 管理中心或 Snort.org。

Snort 规则：41306-41309、41312-41313

发布者：MARTIN LEE 发布时间：14:05

标签：CVE-2016-8732、CVE-2016-9038、CVE-2017-2802、DELL、INVINCEA、漏洞、漏洞聚焦

分享此文