2017 年 5 月 5 日，星期五

漏洞聚焦：Power Software PowerISO 的 ISO 代码执行漏洞

漏洞发现者：思科 Talos 团队的 Piotr Bania。

今天，Talos 发布了在 Power Software PowerISO 磁盘映像软件中发现的新漏洞。当使用 PowerISO 软件打开并解析经特殊设计的 ISO 映像时，攻击者可利用 TALOS-2017-0318 和 TALOS-2017-0324 在易受攻击的系统中远程执行任意代码。

简介

漏洞存在于 Power Software PowerISO 磁盘映像实用程序中，Windows 用户使用该软件创建、编辑、装载和转换各种常见的磁盘映像文件格式。家庭用户通常使用该软件装载 ISO 磁盘映像，因为 Windows 8 之前的版本默认不包含此功能。

ISO (9660) 磁盘映像格式是单个文件中的文件系统。实质上，它是标准软件 CD-ROM 安装磁盘使用的文件系统的二进制副本。如今，常用软件和操作系统的安装磁盘大都使用 ISO 文件格式进行分发。

TALOS-2017-0318 - Power Software PowerISO 的 ISO 代码执行漏洞 (CVE-2017-2817)

堆叠缓冲区溢出漏洞存在于 Power Software Ltd PowerISO 磁盘映像软件的 ISO 映像解析功能中。经特殊设计的 .ISO 文件引发的漏洞可导致潜在的代码执行。攻击者可发送特的 .ISO 文件来触发此漏洞。有关漏洞的更多信息，请参阅报告 TALOS-2017-0318。

TALOS-2017-0324 - PowerISO 的 ISO 解析释放后使用漏洞 (CVE-2017-2823)

释放后使用漏洞存在于 PowerISO 6.8 的 .ISO 解析功能中。经特殊设计的 .ISO 文件引发的漏洞可导致潜在的代码执行。攻击者可发送特定的 .ISO 文件来触发此漏洞。有关所发现的漏洞的更多信息，请参阅报告 TALOS-2017-0324

已知存在漏洞的版本

PowerISO 6.8。

讨论

ISO 9660 文件格式是一种较旧的格式，其原始规范对文件名长度、目录深度以及文件大小上限有一些限制。这些限制继承自较旧版本的操作系统。具体而言，ISO 9660 文件系统中的文件名长度上限为 8 个字符，文件扩展名上限为 3 个字符。

随着时间的推移，人们已开发出各种扩展名来克服原始文件格式规范的限制。其中一个扩展名，即所谓的 Rock Ridge 扩展名，允许原始文件使用替代名称。替代名称的长度可以超过默认的 8 个字符。

在解析替代名称 (NM) 系统用条目时，PowerISO 软件中存在漏洞。替代名称的结构包含一个单字节长度字段，攻击者可利用该字段引发堆栈缓冲区溢出，从而可以在 PowerISO 用户环境中实现远程代码执行。

虽然许多情况下第三方磁盘映像实用程序可能非常有用，但有必要检查默认的操作系统功能是否满足用户需求。具体而言，Windows 8 及更高版本内置了装载 ISO 映像的功能，因而无需使用第三方磁盘映像实用程序。

仍然需要使用第三方磁盘映像软件的用户应确保产品发布安全更新后立即进行应用，以修复潜在的攻击媒介。

防护

以下 Snort 规则可以检测相关的漏洞攻击活动。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：42263-42272 (TALOS-2017-0318)
42321、42322 (TALOS-2017-0324)

发布者：VANJA SVAJCER；发布时间：13:53
标签：CVE-2017-2817、CVE-2017-2823、漏洞研究、漏洞聚焦