2016 年 12 月 13 日，星期二

漏洞聚焦：Joyent SmartOS

漏洞发现者：Tyler Bohan

概述

Talos 公开了 Joyent SmartOS（尤其是 Hyprlofs 文件系统）中的一系列漏洞。SmartOS 是基于一个 Opensolaris 分支的开源虚拟机监控程序。Hyperlofs 是 SmartOS 内存文件系统，允许用户在单个命名空间下从各种不同位置映射文件。此外，hyperlofs 还允许快速轻松地创建新的虚拟文件系统。公开的核心漏洞有 3 个。但是，由于在 32 位和 64 位版本中都发现了这些漏洞，因此总共有 6 个与 6 份 Talos 报告相关的 CVE。

详细信息

TALOS-2016-0248 和 TALOS-2016-0249

该漏洞是由 IOCTL 函数中的整数溢出导致的权限提升漏洞。这与 HYPRLOFS_ADD_ENTRIES 命令尤其相关，并且如果攻击者设计了特定输入，则可以利用此漏洞。所产生的攻击可导致内核错误，或者如果攻击者将 NULL 页映射到用户空间，则会导致权限提升漏洞。有关完整详细信息，请参阅以下报告。
TALOS-2016-0248 / CVE-2016-8733
TALOS-2016-0249 / CVE-2016-9031（32 位）

TALOS-2016-0250 和 TALOS-2016-0252

该漏洞是由 IOCTL 函数中的缓冲区溢出导致的另一个权限提升漏洞。这与 HYPRLOFS_ADD_ENTRIES 命令尤其相关，并且攻击者可以设计特定输入，触发 NM 变量中缓冲区溢出，导致越界内存访问，进而导致权限提升，从而利用此漏洞。有关完整详细信息，请参阅以下报告。
TALOS-2016-0250 / CVE-2016-9032
TALOS-2016-0252 / CVE-2016-9034（32 位）

TALOS-2016-0251 和 TALOS-2016-0253

该漏洞是由 IOCTL 函数中的缓冲区溢出导致的另一个权限提升漏洞。这与 HYPRLOFS_ADD_ENTRIES 命令尤其相关，并且攻击者可以设计特定输入，触发 NM 变量中缓冲区溢出，导致越界内存访问，进而导致权限提升，从而利用此漏洞。有关完整详细信息，请参阅以下报告。
TALOS-2106-0251 / CVE-2016-9033
TALOS-2016-0253 / CVE-2016-9035（32 位）

防护

以下 Snort 规则将会检测出漏洞攻击尝试。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：40898-40903

发布者：NICK BIASINI；发布时间：13:58

标签：零日、披露、漏洞聚焦