2017 年 3 月 7 日，星期二

漏洞聚焦：Pharos 漏洞

漏洞发现者：思科 Talos 团队的 Tyler Bohan。Talos 在此衷心感谢纽约大学 Osiris Lab 帮助修复这些漏洞。

Pharos PopUp Printer 是一款打印软件，广泛用于管理与单一打印点之间的多个连接。以根权限运行并向网络连接开放的服务是吸引攻击者的诱人目标。据 Talos 披露，Pharos PopUp 打印机客户端版本 9.0 的 psnotifyd 应用中存在三个代码执行漏洞和一个拒绝服务漏洞

TALOS-2017-0280、TALOS-2017-0283 代码执行漏洞（CVE-2017-2785、CVE-2017-2788）
TALOS-2017-0282 内存代码执行漏洞 (CVE-2017-2787)
TALOS-2017-0281 DecodeString 拒绝服务漏洞 (CVE-2017-2786)

详细信息

TALOS-2017-0280、TALOS-2017-0283

该应用的 DecodeString 和 DecodeBinary 函数中存在可被利用的缓冲区溢出漏洞。在这两种情况下都可以制作一个恶意数据包（其中包含二进制或字符串数据以及由攻击者控制的描述该数据长度的值），然后将该数据包发送到受害者的计算机。提供超大的数据长度值会导致各自函数中的循环越界写入分配的缓冲区外部，进而导致缓冲区溢出，并最终导致远程代码执行。更多详细信息，请点击此处和此处

TALOS-2017-0282

Blob 数据是建立连接时向客户端返回的编码数据。从攻击者传入的数据可部分控制其开始。BlobData 函数会解析此数据，连续递减寄存器，直到达到该数据包末尾。但是，没有相关检查可防止寄存器递减越过零。如果发生这种情况，memcpy 就会引发越界写入。通过向受害者的计算机同时发起多个连接，就有可能利用此漏洞执行攻击者提供的代码。更多详细信息，请访问此处

TALOS-2017-0281

DecodeString 函数允许将数据长度解码为由数据包中的值提供数据长度。攻击者能够制作一个恶意数据包，提供无效的数据长度值。其结果是指向越界内存位置的无效指针被取消引用。这会导致越界访问和拒绝服务条件。更多详细信息，请访问此处

测试版本

Pharos PopUp 打印机客户端版本 9.0

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：41505 - 41510

发布者：WARREN MERCER；发布时间：11:06