2017 年 5 月 25 日，星期二

Samba 漏洞：悄然滑动脚步，伺机威胁您身边的网络

简介

日前，一个对广泛使用的 Samba 软件造成影响的新漏洞公布于众。Samba 是 *NIX 操作系统中常用的 SMB/CIFS 协议。CVE-2017-7494 有可能影响全世界的许多系统。此漏洞可能会允许用户将共享库上传至易受攻击的 Samba 服务器上的可写共享，并导致服务器执行上传的文件。攻击者可以利用这种方式将漏洞攻击负载上传至可写的 Samba 共享，进而在运行受影响版本的 Samba 软件包的所有服务器上执行代码。目前，此漏洞的影响范围包括所有 Samba 3.5.0 版本（2010 年 3 月发布）及更高版本。为强化攻击带来的严重性并降低实施复杂性，攻击者可能会使用一个 Metasploit 单行指令来触发此漏洞。

旨在解决此问题的补丁已经发布。此外，Samba 自身配置中也具有一项缓解措施。将参数“nt pipe support = no”添加至 smb.conf 文件的全局部分，并重新启动该服务，也可缓解此威胁。此威胁不过暂露头角，刚刚被潜在攻击者利用已在互联网上公布的 POC 代码发现。攻击者开始更广泛地利用此威胁危害外部和内部的更多系统，只是一个时间问题。

这可能会影响许多服务器、存储设备（例如 NAS 系统），以及运行易受此攻击的 Samba 版本的所有其他设备。我们强烈建议用户与其供应商联系，获取相关修复固件或建议，以便应对此威胁。同时，以上解决方案也可帮助应对此威胁。根据最佳实践，我们强烈建议用户不要允许直接 SMB、Samba、CIFS、NFS 等设备从互联网接入至网络内部的系统。

防护

Snort 规则：43002-43004

打开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	生产
AMP	不适用
CloudLock	不适用
CWS	不适用
邮件安全	不适用
网络安全	✔
Threat Grid	不适用
Umbrella	不适用
WSA	不适用

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

StealthWatch 可以检测网络扫描活动、网络传播和与 CnC 基础设施的连接，从而与此活动建立联系，通知管理员。

发布者：NICK BIASINI；发布时间：3:31
标签：SAMBA、TALOS、漏洞