Brendan Dolan-Gavitt
@moyix

Folgen

Looks like I have my first exploit attempt against the Cisco SNMP vuln from the #ShadowBrokers leak!

```
Aug 18 14:24:35 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 69.60.114.130:40064 -> 216.165.113.171:161
moyix@lorenzo:~$
```

RETWEETS 185 GEFÄLLT 159

20:10 - 18. Aug. 2016

Brooklyn, NY

185 159

Brendan Dolan-Gavitt @moyix · 20. Aug.
@moyix Update: two more came early this morning.

```
Aug 20 05:54:48 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:37652 -> 216.165.113.171:161
Aug 20 05:56:24 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:51649 -> 216.165.113.171:161
Aug 20 05:56:41 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:37825 -> 216.165.113.171:161
Aug 20 05:56:45 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:53571 -> 216.165.113.171:161
Aug 20 06:04:18 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:59810 -> 216.165.113.171:161
Aug 20 06:09:48 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 46.209.63.139:59615 -> 216.165.113.171:161
Aug 20 06:22:52 lorenzo snort[1285]: [3:39885:1] PROTOCOL-SNMP Cisco ASA SNMP OID
 parsing stack buffer overflow attempt [Classification: Attempted Administrator P
rivilege Gain] [Priority: 1] {UDP} 167.114.166.245:40673 -> 216.165.113.171:161
moyix@lorenzo:~/CVE-2016-6366$
```

15 7

h4ck_trap @h4ck_tr4p · 19. Aug.
@moyix Thanks for giving us in TSS a mild heart attack today!

3

Brendan Dolan-Gavitt @moyix · 19. Aug.
@nickr01 Ha, sorry about that! Is there a good way to let you guys know next time