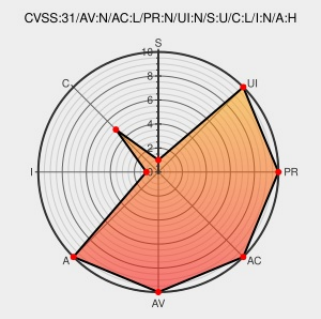
CVE-2019-13030

Published on: 08/14/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

CVE-2019-13030

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Neo Server from Mediola contain the following vulnerability:

eQ-3 Homematic CCU3 AddOn 'Mediola NEO Server for Homematic CCU3' prior to 2.4.5 allows uncontrolled admin access to start or stop the Node.js process, resulting in the ability to obtain mediola configuration details. This is related to improper access control for addons configuration pages and a missing check in rc.d/97NeoServer.

CVE-2019-13030 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	HIGH

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
CVE-2019-13030 eQ-3 Homematic CCU3 AddOn 'Mediola NEO Server for	Exploit Third Party Advisory psytester.github.io	MISC psytester.github.io/CVE-2019-13030/

Homematic CCU3 prior 2.4.5 allows uncontrolled admin access to start or stop the Node.js process, resulting in the ability to obtain mediola configuration details. This is related to improper access control for addons configuration pages and a missing check in rc.d/97NeoServer – psytester – Testing is my passion. Sharing knowledge is my contribution.	text/html	
psytester.github.io/2019-06-29-CVE-2019-13030.md at master · psytester/psytester.github.io · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/psytester/psytester.github.io/blob/master/_posts/hacking_and_pentests/CVEs06-29-CVE-2019-13030.md

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mediola	Neo Server	All	All	All	All
Application	Mediola	Neo Server	All	All	All	All

cpe:2.3:a:mediola:neo_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:mediola:neo_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→