



CVE-2018-18392

Published on: 10/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

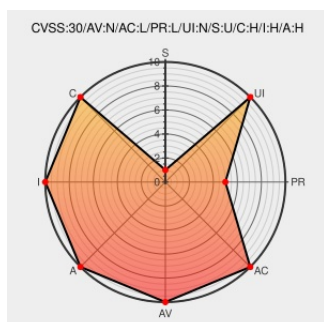
CVE-2018-18392

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Thingspro](#) from [Moxa](#) contain the following vulnerability:

Privilege Escalation via Broken Access Control in Moxa ThingsPro IIoT Gateway and Device Management Software Solutions version 2.1.

CVE-2018-18392 has been assigned by [K](#) vulnerability@kaspersky.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [K](#) **Moxa - ThingsPro IIoT Gateway and Device Management Software Solutions** version 2.1

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
KLCERT-18-020: Moxa ThingsPro IIoT Gateway and Device Management Software Solutions: Broken Access Control Kaspersky ICS CERT	Third Party Advisory ics-cert.kaspersky.com text/html	MISC ics-cert.kaspersky.com/advisories/kcert-advisories/2018/10/18/kcert-18-020-moxa-thingspro-iiot-gateway-and-device-management-software-solutions-

Access Control | Raspberry Pi OS CVE-2023-0166

gateway and device management controls solution broken-access-control/

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	Moxa	Thingspro	2.1	All	All	All
Application	Moxa	Thingspro	2.1	All	All	All

cpe:2.3:a:moxa:thingspro:2.1:*****:

cpe:2.3:a:moxa:thingspro:2.1:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→