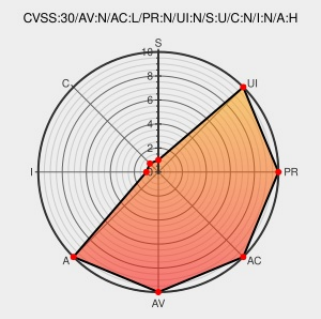
CVE-2020-6084

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 07/29/2022 01:32:00 PM UTC

CVE-2020-6084

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



Certain versions of Flex I/o 1794-aent from Rockwellautomation contain the following vulnerability:

An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less bytes than required by the Key Format Table.

CVE-2020-6084 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
TALOS-2020-1006 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory	MISC talosintelligence.com/vulnerability_reports/TALOS-

talosintelligence.com 2020-1006
text/html

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
Hardware	Rockwellautomation	Flex I/o 1794-aent	-	All	All	All
Hardware	Rockwellautomation	Flex I/o 1794-aent	-	All	All	All
Operating System	Rockwellautomation	Flex I/o 1794-aent	4.003	All	All	All
Operating System	Rockwellautomation	Flex I/o 1794-aent	4.003	All	All	All

cpe:2.3:h:rockwellautomation:flex_i\/o_1794-aent:-:*:*:*:*:*:*:*:

cpe:2.3:h:rockwellautomation:flex_i\/o_1794-aent:-:*:*:*:*:*:*:*:

cpe:2.3:o:rockwellautomation:flex_i\/o_1794-aent:4.003:*:*:*:*:*:*:*:

cpe:2.3:o:rockwellautomation:flex_i\/o_1794-aent:4.003:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID Next ID→