

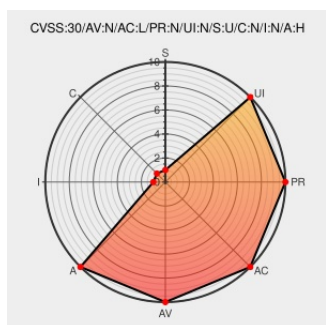


CVE-2020-6086

Published on: 10/14/2020 12:00:00 AM UTC

Last Modified on: 07/29/2022 01:31:00 PM UTC

CVE-2020-6086

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Flex I/o 1794-aent/b](#) from [Rockwellautomation](#) contain the following vulnerability:

An exploitable denial of service vulnerability exists in the ENIP Request Path Data Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. 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. If the

Simple Segment Sub-Type is supplied, the device treats the byte following as the Data Size in words. When this value represents a size greater than what remains in the packet data, the device enters a fault state where communication with the device is lost and a physical power cycle is required.

CVE-2020-6086 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-2020-1007 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	 MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1007

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/b	-	All	All	All
Hardware 	Rockwellautomation	Flex I/o 1794-aent/b	-	All	All	All
Operating System	Rockwellautomation	Flex I/o 1794-aent/b Firmware	4.003	All	All	All
Operating System	Rockwellautomation	Flex I/o 1794-aent/b Firmware	4.003	All	All	All
cpe:2.3:h:rockwellautomation:flex_iVo_1794-aent\b:-:*:*:*:*:*:						
cpe:2.3:h:rockwellautomation:flex_iVo_1794-aent\b:-:*:*:*:*:*:						
cpe:2.3:o:rockwellautomation:flex_iVo_1794-aent\b_firmware:4.003:*:*:*:*:*:						
cpe:2.3:o:rockwellautomation:flex_iVo_1794-aent\b_firmware:4.003:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID→		