



CVE-2018-5442

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-5442
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-05 18:29:00 UTC
Updated	2020-09-18 15:53:00 UTC
Description	A Stack-based Buffer Overflow issue was discovered in Fuji Electric V-Server VPR 4.0.1.0 and prior. The stack-based buffer overflow could allow an attacker to execute arbitrary code or cause a denial of service (crash) on the affected device.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	FujiElectric	V-server Vpr	-	All	All	All
Hardware	FujiElectric	V-server Vpr	-	All	All	All
Operating System	FujiElectric	V-server Vpr Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Fuji Electric V-Server VPR ICS-CERT	MISC	ics-cert.us-cert.gov	Mitigation, Third Party Advisory
Fuji Electric V-Server VPR CVE-2018-5442 Stack Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report