



CVE-2021-20596

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

Summary

CVE	CVE-2021-20596
State	PUBLIC
Assigner	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-22 12:15:00 UTC
Updated	2021-08-02 14:25:00 UTC
Description	NULL Pointer Dereference in MELSEC-F Series FX3U-ENET firmware version 1.14 and prior, FX3U-ENET-L firmware vers

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mitsubishielectric	Fx3u-enet-l Firmware	All	All	All	All
Operating System	Mitsubishielectric	Fx3u-enet-p502 Firmware	All	All	All	All
Operating System	Mitsubishielectric	Fx3u-enet Firmware	All	All	All	All

References

Reference	Source
www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-006_en.pdf	MISC
Mitsubishi Electric MELSEC-F Series CISA	MISC
JVNVU#94348759: 三菱電機製 MELSEC F シリーズ Ethernet インタフェースブロックにおける NULL ポインタ参照の脆弱性	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590654](#) Mitsubishi Electric MELSEC-F Series Denial of Service (DoS) Vulnerability (ICSA-21-201-01)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)