



CVE-2021-20606

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

Summary

CVE	CVE-2021-20606
State	PUBLIC
Assigner	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-17 17:15:00 UTC
Updated	2023-02-02 19:55:00 UTC
Description	Out-of-bounds Read vulnerability in Mitsubishi Electric GX Works2 versions 1.606G and prior, Mitsubishi Electric MELSOFT

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mitsubishielectric	Ezsocket	All	All	All	All
Application	Mitsubishielectric	Ezsocket	All	All	All	All
Application	Mitsubishielectric	Gx Works2	All	All	All	All
Application	Mitsubishielectric	Melsoft Navigator	All	All	All	All

References

Reference	Source	Link	Ta
JVNVU#93817405: 三菱電機製FAエンジニアリングソフトウェア製品における複数の脆弱性	MISC	jvn.jp	
Mitsubishi Electric FA Engineering Software CISA	MISC	us-cert.cisa.gov	
www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-021_en.pdf	MISC	www.mitsubishielectric.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590657](#) Mitsubishi Electric FA Engineering Software Multiple Vulnerabilities (ICSA-21-350-05)

© [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](#)