



CVE-2023-3373

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

Summary

CVE	CVE-2023-3373
State	PUBLIC
Assigner	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-04 00:15:00 UTC
Updated	2023-08-10 14:59:00 UTC
Description	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT21 model

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mitsubishielectric	Gs21	-	All	All	All
Operating System	Mitsubishielectric	Gs21 Firmware	All	All	All	All
Hardware	Mitsubishielectric	Gt21	-	All	All	All
Operating System	Mitsubishielectric	Gt21 Firmware	All	All	All	All

References

Reference

Mitsubishi Electric GOT2000 and GOT SIMPLE | CISA

JVNVU#92167394: 三菱電機製GOT2000シリーズおよびGOT SIMPLEシリーズのFTPサーバ機能にデータコネクションを待ち受けるポート

www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-006_en.pdf

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#)