



Information Tampering Vulnerability in Multiple Processes of GENESIS64, ICONICS Suite, MobileHMI, Hyper Historian, AnalytiX, IoTWorX, MC Works64, and GENESIS

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

Summary

CVE	CVE-2025-7376
State	PUBLISHED
Assigner	Mitsubishi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-06 07:15:34 UTC
Updated	2026-04-09 06:16:22 UTC
Description	Windows Shortcut Following (.LNK) vulnerability in multiple processes of Mitsubishi Electric GENESIS64 versions 10.97.3 a

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp

CVSS: 3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N

EPSS: 0.000140000 probability, percentile 0.026280000 (date 2026-04-13)

Problem Types: CWE-64 | CWE-64 CWE-64 Windows Shortcut Following (.LNK)

Version	Source	Type	Score	Severity	Vector
3.1	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp	Secondary	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mitsubishi Electric Corporation	GENESIS64	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	GENESIS64	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Corporation	ICONICS Suite	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	ICONICS Suite	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Corporation	MobileHMI	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	MobileHMI	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Corporation	Hyper Historian	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	Hyper Historian	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Corporation	AnalytiX	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	AnalytiX	affected versions 10.97.3 and prior	Not specified
CNA	Mitsubishi Electric Corporation	IoTWorkX	affected version 10.95	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	IoTWorkX	affected version 10.95	Not specified
CNA	Mitsubishi Electric Corporation	MC Works64	affected all versions	Not specified
CNA	Mitsubishi Electric Corporation	GENESIS	affected version 11.00	Not specified
CNA	Mitsubishi Electric Iconics Digital Solutions	GENESIS	affected version 11.00	Not specified

References

Reference	Source	Link
www.cisa.gov/news-events/ics-advisories/icsa-25-217-01	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp	www.cisa.gov
jvn.jp/vu/JVNVU96364629	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp	jvn.jp
www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-009_en.pdf	Mitsubishielectric.Psirt@yd.MitsubishiElectric.co.jp	www.mitsubishielectric.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

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