America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update B)

Last Revised: April 07, 2026 **Alert Code:** ICSA-25-217-01

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2025/icsa-25-217-01_drupal.json>

Summary

Successful exploitation of this vulnerability could allow a local attacker to make an unauthorized write to arbitrary files, by creating a symbolic link from a file used as a write destination by the processes of the affected products to a target file. This could

allow the attacker to destroy the file on a PC with the affected products installed, resulting in a denial-of-service (DoS) condition on the PC if the destroyed file is necessary for the operation of the PC.

The following versions of Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update B) are affected:

- Mitsubishi Electric GENESIS64 <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric ICONICS Suite <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric MobileHMI <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Hyper Historian <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric AnalytiX <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric IoTWorX 10.95 (CVE-2025-7376)
- Mitsubishi Electric MC Works 64 vers:all/* (CVE-2025-7376)
- Mitsubishi Electric GENESIS 11.00 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions GENESIS64 <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions ICONICS Suite <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions MobileHMI <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions Hyper Historian <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions AnalytiX <=10.97.3 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions IoTWorX 10.95 (CVE-2025-7376)
- Mitsubishi Electric Iconics Digital Solutions GENESIS 11.00 (CVE-2025-7376)

CVSS	Vendor	Equipment	Vulnerabilities
v3 5.9	Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric	Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update B)	Windows Shortcut Following (.LNK)

Background

- **Critical Infrastructure Sectors:** Critical Manufacturing
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** United States, Japan

Vulnerabilities

Expand All +

CVE-2025-7376 +

Acknowledgments

- Mitsubishi Electric reported these vulnerabilities to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (https://www.cisa.gov/notification) and this Privacy & Use policy (https://www.cisa.gov/privacy-policy).

Recommended Practices

CISA recommends users take defensive measures to minimize the exploitation risk of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolate them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most recent version available. Also recognize VPN is only as secure as its connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

Advisory Conversion Disclaimer

This ICSA is a verbatim republication of Mitsubishi Electric 2025-009 from a direct conversion of the vendor's Common Security Advisory Framework (CSAF) advisory. This is republished to CISA's website as a means of increasing visibility and is provided "as-is" for informational purposes only. CISA is not responsible for the editorial or technical accuracy of republished advisories and provides no warranties of any kind regarding any information contained within this advisory. Further, CISA does not endorse any commercial product or service. Please contact Mitsubishi Electric directly for any questions regarding this advisory.

Revision History

- **Initial Release Date:** 2025-08-05

Date	Revision	Summary
2025-08-05	1	Initial Publication

Date	Revision	Summary
2025-09-04	2	Update A - Modified the vulnerability description in section 3.2.1 to clarify the privilege level required by the attacker, modified the company name in section 4.0 to Mitsubishi Electric Iconics Digital Solutions, and added a statement from Mitsubishi regarding a patched version of GENESIS64 that is in development.
2026-04-07	3	Update B - Added MobileHMI, Hyper Historian, AnalytiX, and IoTWorX as affected products, and added information on affected versions and vendor fix for GENESIS64, GENESIS, MobileHMI, Hyper Historian, AnalytiX, and IoTWorX.

Legal Notice and Terms of Use

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- ICONICS, Mitsubishi Electric

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-03

Anviz Multiple Products </news-events/ics-advisories/icsa-26-106-03>

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-04

AVEVA Pipeline Simulation </news-events/ics-advisories/icsa-26-106-04>

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-01

Delta Electronics ASDA-Soft </news-events/ics-advisories/icsa-26-106-01>

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-02

Horner Automation Cscape and XL4, XL7 PLC </news-events/ics-advisories/icsa-26-106-02>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security