An official website of the United States government Here's how you know

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric Iconics Digital Solutions / Mitsubishi Electric GENESIS64 (Update F)

Last Revised: April 07, 2026 **Alert Code:** ICSA-25-140-04

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-25-140-04_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 services of the affected products to a target file, enabling the

attacker to destroy the file on a PC with affected products installed and thereby cause 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 and Mitsubishi Electric Products (Update F) are affected:

- Mitsubishi Electric GENESIS64 <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric ICONICS Suite <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric MobileHMI <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Hyper Historian <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric AnalytiX <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric IoTWorX 10.95 (CVE-2025-0921)
- Mitsubishi Electric GENESIS32 vers:all/* (CVE-2025-0921)
- Mitsubishi Electric BizViz vers:all/* (CVE-2025-0921)
- Mitsubishi Electric GENESIS 11.00 (CVE-2025-0921)
- Mitsubishi Electric MC Works64 vers:all/* (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions GENESIS64 <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions ICONICS Suite <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions MobileHMI <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions Hyper Historian <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions AnalytiX <=10.97.3 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions IoTWorX 10.95 (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions GENESIS32 vers:all/* (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions BizViz vers:all/* (CVE-2025-0921)
- Mitsubishi Electric Iconics Digital Solutions GENESIS 11.00 (CVE-2025-0921)

CVSS	Vendor	Equipment	Vulnerabilities
v3 6.5	Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric	Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update F)	Execution with Unnecessary Privileges

Background

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

Vulnerabilities

Expand All +

CVE-2025-0921 +

Acknowledgments

- Asher Davila of Palo Alto Networks reported this vulnerability to Mitsubishi Electric and CISA
- Malav Vyas of Palo Alto Networks reported this vulnerability to Mitsubishi Electric and 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 2025-002 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:** 2025-05-20

Date	Revision	Summary
2025-05-20	1	Initial Publication

Date	Revision	Summary
2025-08-07	2	Update A - Removed AlarmWorX64 wording from the Affected Products section, added reference to other services in the vulnerability overview, removed the multi-agent service disablement mitigation action, and updated CVE description and CVSS score.
2025-08-28	3	Update B - Modified company name to "Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric" and added a statement from Mitsubishi regarding a patched version of GENESIS64 that is in development.

Date	Revision	Summary
2026-01-08	4	Update C - Added BizViz and GENESIS32 as affected products, added GENESIS32 and BizViz to the vulnerability description, and added relevant mitigations strategies for GENESIS32 and BizViz as requested by Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric
2026-01-29	5	Update D - Added ICONICS Suite to the affected products list and adjusted the brand name of MC Works64 to Mitsubishi Electric MC Works64
2026-02-12	6	Update E - Updated product list to correct vendor associations in the CSAF

Date	Revision	Summary
2026-04-07	7	Update F -Added MobileHMI, Hyper Historian, AnalytiX, and IoTWorX as affected products, and added information on affected versions and vendor fix for GENESIS64, ICONICS Suite, 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
- 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 09, 2026 ■ ICS ADVISORY | ICSA-26-099-02

GPL Odorizers GPL750 </news-events/ics-advisories/icsa-26-099-02>

APR 09, 2026 ■ ICS ADVISORY | ICSA-26-099-01

Contemporary Controls BASC 20T </news-events/ics-advisories/icsa-26-099-01>

APR 07, 2026 ■ ICS ADVISORY | ICSA-26-097-01

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-02

Mitsubishi Electric GENESIS64 and ICONICS Suite products

</news-events/ics-advisories/icsa-26-097-01>

Yokogawa CENTUM VP </news-events/ics-advisories/icsa-26-092-02>

Return to top