America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update D)

Last Revised: April 07, 2026 **Alert Code:** ICSA-24-184-03

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/2024/icsa-24-184-03_drupal.json>

Summary

Successful exploitation of these vulnerabilities could result in denial-of-service, improper privilege management, or potentially arbitrary code execution.

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

- Mitsubishi Electric Iconics Digital Solutions ICONICS Suite 10.97.2, <=10.97.2, <=10.97.3 (CVE-2023-2650, CVE-2023-4807, CVE-2024-1573, CVE-2024-1574, CVE-2024-1182)
- Mitsubishi Electric Iconics Digital Solutions GENESIS64 10.97.2, <=10.97.2, <=10.97.3 (CVE-2023-2650, CVE-2023-4807, CVE-2024-1573, CVE-2024-1574, CVE-2024-1182)
- Mitsubishi Electric Iconics Digital Solutions AnalytiX 10.97.2, <=10.97.2, <=10.97.3, 10.97.2, <=10.97.2 (CVE-2023-2650, CVE-2023-4807, CVE-2024-1573, CVE-2024-1574, CVE-2024-1182, CVE-2023-2650, CVE-2023-4807, CVE-2024-1573, CVE-2024-1574)
- Mitsubishi Electric Iconics Digital Solutions MobileHMI 10.97.2, <=10.97.2 (CVE-2023-2650, CVE-2023-4807, CVE-2024-1573, CVE-2024-1574)
- Mitsubishi Electric Iconics Digital Solutions GENESIS32 <=9.7 (CVE-2024-1182, CVE-2024-1574)
- Mitsubishi Electric Iconics Digital Solutions BizViz <=9.7 (CVE-2024-1574)
- Mitsubishi Electric Iconics Digital Solutions IoTWorX 10.95 (CVE-2024-1573)

CVSS	Vendor	Equipment	Vulnerabilities
v3 7	Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric	Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update D)	Allocation of Resources Without Limits or Throttling, Improper Verification of Cryptographic Signature, Uncontrolled Search Path Element, Missing Authentication for Critical Function, Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')

Background

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

Vulnerabilities

Expand All +

CVE-2023-2650 +

CVE-2023-4807 +

CVE-2024-1182 +

CVE-2024-1573 +

CVE-2024-1574 +

Acknowledgments

- Asher Davila and Malav Vyas of Palo Alto Networks reported CVE-2024-1182 to Mitsubishi Electric Iconics Digital Solutions.

Legal Notice and Terms of Use

Recommended Practices

CISA recommends users take defensive measures to minimize the exploitation risk of this vulnerability. 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 2024-004 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. Contact CISA directly for any questions regarding this advisory.

Revision History

- **Initial Release Date:** 2024-07-02

Date	Revision	Summary
2024-07-02	1	Initial Publication
2024-12-03	2	Update A - Added Mitsubishi Electric MC Works64, re-categorized CVE-2023-4807 as CWE-347.
2026-01-08	3	Update B - Added GENESIS32.
2026-03-03	4	Update C - Fixes for affected versions and typographical errors
2026-04-07	5	Update D - Added Hyper Historian, AnaltitiX, and MobileHMI for affected products

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

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

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

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