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 GENESIS64 and ICONICS Suite products

Release Date: April 07, 2026 **Alert Code:** ICSA-26-097-01

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/2026/icsa-26-097-01.json>

Summary

Successful exploitation of these vulnerabilities could allow a local attacker to disclose SQL Server credentials used by the affected products and use them to disclose, tamper with, or destroy data, or to cause a denial-of-service (DoS) condition on the system.

The following versions of Mitsubishi Electric GENESIS64 and ICONICS Suite products are affected:

- GENESIS64 <=10.97.3 (CVE-2025-14815, CVE-2025-14816)
- ICONICS Suite <=10.97.3 (CVE-2025-14815, CVE-2025-14816)
- MobileHMI <=10.97.3 (CVE-2025-14815, CVE-2025-14816)
- Hyper Historian <=10.97.3 (CVE-2025-14815, CVE-2025-14816)
- AnalytiX <=10.97.3 (CVE-2025-14815, CVE-2025-14816)
- MC Works 64 vers:all/* (CVE-2025-14815, CVE-2025-14816)
- GENESIS <=11.02 (CVE-2025-14815, CVE-2025-14816)

CVSS	Vendor	Equipment	Vulnerabilities
v3 8.8	Mitsubishi Electric	Mitsubishi Electric GENESIS64 and ICONICS Suite products	Cleartext Storage of Sensitive Information, Cleartext Storage of Sensitive Information in GUI

Background

- **Critical Infrastructure Sectors:** Critical Manufacturing
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** Mitsubishi Electric Iconics Digital Solutions is headquartered in the United States. Mitsubishi Electric is headquartered in Japan.

Vulnerabilities

Expand All +

CVE-2025-14815 +

CVE-2025-14816 +

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 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 CISA V20251021-001, V20251029-001 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 CISA directly for any questions regarding this advisory.

Revision History

- **Initial Release Date:** 2026-04-07

Date	Revision	Summary
2026-04-07	1	Initial Publication
2026-04-07	2	Initial CISA Republication of CISA V20251021-001, V20251029-001 advisory

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 02, 2026 ■ ICS ADVISORY | ICSA-26-092-01

Siemens SICAM 8 Products </news-events/ics-advisories/icsa-26-092-01>

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

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

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-03

Hitachi Energy Ellipse </news-events/ics-advisories/icsa-26-092-03>

MAR 31, 2026 ■ ICS ADVISORY | ICSA-26-090-01

Anritsu Remote Spectrum Monitor </news-events/ics-advisories/icsa-26-090-01>

Return to top

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>