ICS Advisory (ICSA-22-207-01)

More ICS-CERT Advisories

Inductive Automation Ignition (Update A)

Original release date: August 04, 2022

Legal Notice

1. EXECUTIVE SUMMARY

- CVSS v3 8.5
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Inductive Automation
- **Equipment:** Ignition
- **Vulnerability:** Improper Restriction of XML External Entity Reference

2. UPDATE INFORMATION

This updated advisory is a follow-up to the advisory update titled ICSA-22-207-01 Inductive Automation Ignition that was published July 26, 2022, to the ICS webpage at www.cisa.gov/ics

3.RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to obtain file contents.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following versions of Inductive Automation Ignition software are affected:

-------- **Begin Update A Part 1 of 1** ---------

- Inductive Automation Ignition: All versions from 8.1 to those prior to v8.1.8
- Inductive Automation Ignition: All 7.9 versions prior to v7.9.21

--------- **End Update A Part 1 of 1** ---------

4.2 VULNERABILITY OVERVIEW

4.2.1 IMPROPER RESTRICTION OF XML EXTERNAL ENTITY REFERENCE CWE-611

Due to an XML external entity reference, the software parses XML in the backup/restore functionality without XML security flags, which may lead to a XXE attack while restoring the backup.

CVE-2022-1704 has been assigned to this vulnerability. A CVSS v3 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L).

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing, Energy, Information Technology
- **COUNTRIES/AREAS DEPLOYED:** United States
- **COMPANY HEADQUARTERS LOCATION:** United States

4.4 RESEARCHER

Keval Shah reported this vulnerability to CISA.

5. MITIGATIONS

Inductive Automation recommends users upgrade the Ignition software to the latest version:

- Inductive Automation Ignition: Version 8.1.9 or later
- Inductive Automation Ignition: Version 7.9.21 or later

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability these vulnerabilities. Specifically, users should:

- 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 secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current 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 at cisa.gov/ics. 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.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics 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.

No known public exploits specifically target this vulnerability.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.
