ICS Advisory (ICSA-22-102-03)

More ICS-CERT Advisories

Inductive Automation Ignition

Original release date: April 12, 2022

Legal Notice

1. EXECUTIVE SUMMARY

- **CVSS v3 6.8**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Inductive Automation
- **Equipment:** Ignition
- **Vulnerability:** Path Traversal

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an authenticated attacker with network access to execute code by uploading a malicious zip file.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Inductive Automation Ignition software are affected:

- Inductive Automation Ignition: All 8.0 versions after 8.0.4
- Inductive Automation Ignition: All 8.1 versions prior to 8.1.10

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL') CWE-22

The affected product may allow an attacker with access to the Ignition web configuration to run arbitrary code.

CVE-2022-1264 has been assigned to this vulnerability. A CVSS v3 base score of 6.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N).

3.3 BACKGROUND

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

3.4 RESEARCHER

Mashav Sapir of Claroty reported this vulnerability to CISA.

4. MITIGATIONS

Inductive Automation recommends users upgrade the Ignition software to 8.1.10 or later.

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

- Ensure the least-privilege user principle is followed.
- 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 the business network.
- 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 on cisa.gov. Several recommended 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 on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

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.
