ICS Advisory (ICSA-CNAVTCS2022001)

1. EXECUTIVE SUMMARY

- **CVSS v3.1- Medium**
- **ATTENTION:** Requires high skill level and attack complexity
- **Vendor:** Emerson
- **Equipment:** AVENTICS AF2 Series flow sensor with Ethernet communication interface
- **Vulnerabilities:** Uncontrolled Resource Consumption and Failure to Restrict URL Access

2. RISK EVALUATION

Emerson has recently identified that the AVENTICS AF2 Series flow sensor with Ethernet communication interface has multiple, specific cybersecurity vulnerabilities. The vulnerabilities may allow attackers to disrupt the embedded web server of the device under very specific circumstances and could allow denial of view functions and possibly exposure of system resources. Such web server disruptions depend on the specific device vulnerability exploited or if the system is compromised. Although integrated web server may be disrupted the measuring capabilities of the sensor algorithm is not affected and will keep functioning. Only display capabilities are affected. Following industry-recommended secure architecture guidelines and applying defense-in-depth measures can help protect these devices from attackers attempting to exploit the vulnerabilities.

3. TECHNICAL DETAILS

Emerson has reviewed the vulnerabilities and has identified that impact to the AVENTICS AF2 Series flow sensor with Ethernet communication interface to be a medium vulnerability (as defined by CVSS v3.1 scoring scale) and is limited to the specific listed vulnerabilities below.

CVE ID	Description	CVSS v3.1 Score	Recommended Mitigation
2021-32503	Uncontrolled Resource Consumption	5.8	Network segmentation / Firewall
2020-32504	Failure to Restrict URL Access	5.3	Network segmentation / Firewall

3.1 AFFECTED PRODUCTS

AVENTICS AF2 Series Flow Sensors with Ethernet communication. Part numbers:

R412026837, R412027179, R412026838, R412027180, R412026839, R412027181 with firmware 1.x and 2.x

3.2 VULNERABILITY OVERVIEW

3.2.1 (CVE-2021-32503) UNCONTROLLED RESOURCE CONSUMPTION
The integrated web server of the AF2 can become non-responsive when exposed to a specially crafted IP packet. The sensor will still be functional and will measure flow, even if the web server is not responding. Only web server functionality is affected. Maintenance level privileges are required to exploit this vulnerability.
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H

3.2.2 CVE-2021-32504 FAILURE TO RESTRICT URL ACCESS
In very specific situations an unauthenticated user could gain access to web URLs that are normally restricted to maintenance level users. This type of attack vector could expose system resources.
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Multiple
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Germany

3.4 RESEARCHER

Emerson identified vulnerabilities based on internal penetration testing.

4. MITIGATIONS

Emerson recommends that customers follow industry best practices for network segmentation and avoid exposing the AF2 product directly to the internet. In addition, a firewall should always be used when making external connections.

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

- Minimize network exposure for all control system devices and/or systems and ensure that 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 that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the 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 us-cert.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 us-cert.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.

No known public exploits specifically targeted these vulnerabilities. A high skill level and specific knowledge of programming languages such as HTML, Java, Python, and other low level embedded coding practices are needed to exploit the vulnerabilities.

Contact Information

If you have questions about this advisory and your particular use case, please contact your local Aventics Impact Partner or Aventics Sales Office. You can also contact Aventics Technical Support at US 877-686-2343. For customers outside of the US, please use the following link for International Toll-free Numbers.