EnerSys
2366 Bernville Road
Reading, PA 19605

800-863-3364
support@alpha.com
www.enersys.com

Date: May 09, 2025

Subject: CVE-2024-12442

Vulnerability Name: Single Webpage (Network Diagnostics) RCE Vulnerability

Vulnerability Type: Remote Code Execution (RCE)

Information: https://www.enersys.com/security/cve-disclosures

Summary

This vulnerability exists on the Network Diagnostics webpage of Alpha XM3.1 and AGW devices and may allow unauthenticated remote code execution.

Affected Products

The following table lists the products impacted by the issue listed above.

Product	Fix Version	Release Date
XM3.1-HP 910-918	V1.10.01	01/24/2025
XM3.1-HP 903-905	V1.10.01	01/24/2025
SMG-HP	V02.07.01	12/12/2024
ADOM	V02.07.01	12/12/2024

Recommended Actions

1. Upgrade XM3.1-HP Firmware Immediately:
    - Current version v1.10.00: Urgent update to v1.10.01
2. Upgrade SMG-HP & ADOM Firmware Immediately:
    - Current version v02.07.00: Urgent update to v02.07.01
3. Contact EnerSys to obtain IOCs and TTPs.
4. Harden Network Configurations:
    - Isolate management interfaces.
    - Restrict access via firewall to trusted IPs.

Disclosure & CVE Policy

EnerSys is following the CVE Program's 90-day disclosure policy. Full CVE details will be published on May 09, 2025.

Credits

EnerSys acknowledges the collaboration of its third-party cybersecurity partner in researching and remediating this issue.

Support & Contact

Technical Support: support@alpha.com
Phone: 1-800-863-3364