EnerSys
2366 Bernville Road
Reading, PA 19605

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

**Date:** May 09, 2025

**Subject:** CVE-2024-11861

**Vulnerability Name:** Web Interface Vulnerability

**Vulnerability Type:** Remote Code Execution (RCE)

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

## Summary

This vulnerability permits remote shell access via the web interface, allowing an entity to execute unauthorized code on the unit.

## Affected Products

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

| Product | Fix Version | Release Date |
|---|---|---|
| XM3.1-HP 910-918 | V1.06.00 | September 2022 |
| XM3.1-HP 903-905 | V1.06.00 | September 2022 |
| SMG-HP | V02.02.00 | December 2022 |
| ADOM | V02.02.00 | December 2022 |

## Recommended Actions

1. Upgrade XM3.1 Firmware Immediately:
    - Current version v1.05 or earlier: Urgent update to v1.07.00 or v1.10.01
    - Current version v1.06: Best effort update to v1.10.01
2. Upgrade SMG-HP & ADOM Firmware Immediately:
    - Current version v02.00.01 or earlier: Urgent update to v02.02.00 or 02.07.01
    - Current version v02.02.00: Best effort 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 by 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