Atop Product Cybersecurity Advisory

EHG2408 / EHG2408-2SFP

Stack buffer overflow vulnerabilities

1. Summary:

Published Date	October 17, 2025	**Last Updated**	October 17, 2025
Severity	High	**CVSS**	8.0
Product	EHG2408/EHG2408-2SFP		
Vulnerability	Stack buffer overflow vulnerabilities		
Corrected	Yes	**Workaround**	No

2. Affected Products:

Product	**Version**
EHG2408/EHG2408-2SFP	Version prior to v3.36

3. Vulnerability Overview

Severity	**Score**	**Vector**	**Type**	**CVE reference**
High	8.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N	Stack overflow	CWE-121

4. Acknowledgements

- Reporter: Daniel Hulliger (daniel.hulliger@armasuisse.ch), Vulnerability Researcher of Cyber-Defense Campus.
- Atop would like to express our appreciation to the reporter for reporting the vulnerability, working with use to help enhance the security of our products, and provide a better service to our customers.

5. Mitigation

Product	Mitigations	Download Link
EHG2408/EHG2408-2SFP	Download and upgrade the firmware	Atop Website.

6. Temporary Mitigation

If firmware upgrade cannot be applied immediately:

- Restrict HTTPs access to trusted management networks.
- Enable management VLAN to a specified port only.
- Using VPN to access the switch.

7. General Recommendations

- Don’t click on untrusted links or open unsolicited attachments in e-mails.
- Backup the configuration before upgrading.
- When remote access is required, use a secure access method, such as a VPN.

8. Contact Us

Mail to: PSIRT@atop.com.tw