Vulnerability disclosure policy

In accordance with security recommendations, Hyosung Heavy Industries Corporation establishes appropriate procedures for handling security vulnerabilities in its products and services. In addition, we periodically monitor public vulnerability databases and conduct penetration testing.

This page summarizes our vulnerability disclosure policy.

Report Vulnerability

Hyosung Heavy Industries Corporation welcomes reports from all individuals who help strengthen the security of our services. To ensure a safe reporting process, please submit your reports in accordance with the guidelines below.

As a good-faith reporter, we kindly ask that you comply with the following guidelines:

- Please conduct only the minimum verification necessary to demonstrate the vulnerability. Any modification, deletion, or downloading of actual user data is strictly prohibited.
- Avoid any testing that could cause system downtime, service degradation, or otherwise impact regular users.
- Please keep the reported vulnerability confidential and do not disclose it to third parties or the public until Hyosung Japan has completed its analysis and official patch.

For reporters who submit vulnerabilities in good faith and follow the guidelines above, we guarantee that no civil or criminal legal actions will be pursued. Hyosung Heavy Industries Corporation respects and protects your valuable efforts.

Please submit your report via the Customer Inquiry link below. We recommend including the following details:

- Contact details of the reporter
- System specs (e.g., product name, firmware version)
- Error symptoms or associated logs
- Technical details (e.g., steps to trigger the vulnerability, sample packet captures)

Contact Us: https://www.hyosung.co.jp/en/contact/

Response Process

Hyosung Heavy Industries Corporation handles received vulnerabilities promptly and transparently according to the following steps

Step 1. Receipt & Acknowledgment [Within 5 business days of receipt]

- Once the report is successfully received, the coordinator will send an acknowledgment email to the reporter.

Step 2. Analysis & Verification [Within 10 business days of receipt]

- The internal department verifies whether the vulnerability can be reproduced, assesses the risk level (based on CVSS metrics, etc.) and determines if it is a valid vulnerability.

Step 3. Remediation & Patching [Timeline varies based on severity]

- The product development department and the product security team collaborate to develop and apply the vulnerability patch.
- However, because each security vulnerability is unique, we cannot guarantee a specific resolution timeline. Remediation actions may include software modifications, new product version releases, and/or updates to security guidelines. Throughout the entire process, we will continuously coordinate with the vulnerability discoverer and affected vendors to ensure all concerns are resolved before the patch is finalized.

Step 4. Result Sharing & Completion

- Upon successful remediation, the results will be shared with the reporter and published on our official website.

Recent Security Updates

Category	Patch Version	Affected Products	CVE	CVSS	Last Update
ESS	3.04.02 3.03.02 3.02.02 3.01.02	HS-EM4200GLO HS-EM3000GLO HS-EM2625GLO HS-EM1500GLO	CVE-2023-48795	7.5	26.06.05
ESS	3.03.01	HS-EM3000GLO			26.05.15
ESS	3.01.01	HS-EM1500GLO			26.05.15
ESS	3.02.01	HS-EM2625GLO			26.05.06
ESS	3.04.01	HS-EM4200GLO			26.05.06