Vulnerability Handling

eucc@gmv.com

GMV has implemented a strategic plan to manage and monitor the cybersecurity of the GMV GNSS Cryptographic Module, for at least 5 years, which includes the following support channels:

1. Vulnerability publication channel. Any new vulnerability identified in the module will be analysed and published in the NIST National Vulnerability Database (NVD).

2. Communication channel. A specific communication channel through the email eucc@gmv.com, where end users and researchers can report vulnerabilities or request additional information about the security of the product.

3. Updates delivery. Product updates and patches will be submitted by GMV to final users when available. GMV GNSS Cryptographic Module users can also request to eucc@gmv.com such updates and patches at any given time.