Vulnerability in Advantech Products

Background
CSA has issued a CVE ID (CVE-2026-6888) to a vulnerability in Advantech products. The product owner, Advantech, an IoT intelligent systems and embedded platform service provider, has released security updates to address it.

Impact
Successful exploitation of the SQL injection vulnerability could allow a remote authenticated attacker to execute arbitrary commands via a specific interface, potentially enabling the attacker to access, modify, or delete sensitive information within the database.

Affected Products
The vulnerability affects the following Advantech products:

- SaaS Composer prior to version 3.4.17
- IoTSuite Growth Linux docker prior to version 2.2.0
- IoTSuite Starter Linux docker prior to version 2.2.0
- IoT Edge Linux docker prior to version 2.2.0
- IoT Edge Windows prior to version 2.2.0
- WebAccess/SCADA prior to version 9.2.3
- WebAccess SaaS-Composer prior to version 3.4.17.1
- ECOWatch SaaS-Composer prior to version 3.4.17

Mitigation
Users and administrators of affected product versions are advised to update to the latest versions immediately.

For SaaS Composer, IoTSuite Growth Linux docker, IoT Edge Windows, and ECOWatch please contact Advantech here for the official release of the fixed version.

For IoTSuite Starter Linux docker, please refer to the update guide here. As the update involves a reinstallation process, please refer to the reinstallation guide here.

For IoT Edge Linux docker, please refer to the update guide here. As the update involves a reinstallation process, please refer to the reinstallation guide here.

For WebAccess/SCADA and WebAccess SaaS-Composer, please refer to the update guide here.

Special Thanks to:

- Informer: Hoa Ly Van Huu, HCMUTE Information Security Club

- Product Owner: Advantech

References
https://www.advantech.com/en/security-advisory
Informer's link (if any)