

EDAN Coordinated Vulnerability Disclosure Statement

EDAN prioritizes "safety and reliability" in the design, manufacturing and full-life-cycle maintenance of medical devices. Upholding an open and collaborative approach, we are committed to building trusted partnerships with the global community of security researchers to jointly verify and respond to all legally disclosed security vulnerabilities. We value the work of security researchers and encourage them to cooperate proactively with us in a coordinated and responsible manner to communicate about identified vulnerabilities and proposed disclosures with us and other relevant parties.

Scope

This coordinated disclosure process is developed exclusively for security researchers to report potential cybersecurity vulnerabilities associated with EDAN's commercial products.

Important note: This process does not provide technical support for EDAN products, nor does it accept reports of adverse events or product quality complaints. For the aforementioned matters, please follow the official designated channels at: <https://www.edandiagnostics.com/service/>.

Submission Method

If you identify potential cybersecurity vulnerabilities related to EDAN products, please contact us via our dedicated email in Chinese or English: security@edan.com. To ensure the security of vulnerability information transmission, we recommend encrypting your email content with the GPG (GnuPG) public key before sending.

Please include the following information in your submission

Contact details for follow-up communication, including name, organization, email address and phone number.

The date and location where the vulnerability was discovered.

A technical description of the vulnerability and its discovery environment.

Detailed information about the affected product, including name, version and configuration.

The specific impacts of the vulnerability and your assessment of how it could potentially be exploited for malicious attacks.

Information about the tools and techniques used to discover the vulnerability.

Any proof-of-concept code or exploit code related to the vulnerability.

Evidence (if any) of the vulnerability being exploited.

Information about any prior or intended disclosure of the vulnerability to third parties (e.g., regulatory authorities, vulnerability coordinators, suppliers).

Please do not include any personal information such as sensitive or health-related data.

What EDAN Will Do

We will confirm receipt of your report within 7 working days.

We will forward the report to the relevant team for vulnerability verification and reproduction. You may be contacted to assist with our validation work during this period. We will assess the vulnerability and conduct a risk analysis to determine the appropriate course of action.

Additional Guidelines for Security Researchers:

Testing must only be conducted in a secure environment that meets all of the following criteria:

Strictly comply with all applicable laws, regulations and industry regulatory requirements of the country/region where the testing is conducted.

Testing activities must not pose any potential risks to patient safety, infringe on personal privacy, or damage the hardware and software systems of the devices.

Testing is strictly prohibited on devices in clinical use (providing diagnosis and treatment services to patients) or in production environments (including officially deployed software and servers).

Only verification of the existence of vulnerabilities is permitted; aggressive actions such as exploiting vulnerabilities to obtain data, take control of devices, or interfere with normal operations are strictly forbidden.

Upon completion of testing, no actions that may alter the original configuration or functional status of the product or system shall be taken, and the integrity of the device/system must be maintained.

Important Notes:

By submitting relevant information through this process, you agree that such information shall be deemed non-proprietary and non-confidential. EDAN may use, modify, disseminate and share all or part of the information for legitimate purposes such as cybersecurity protection and product optimization, without any restrictions on use. At the same time, you confirm that the submission of such information does not constitute an infringement of any statutory or contractual rights owned by EDAN, nor shall it give rise to any express or implied obligations of EDAN to you.

We fully recognize that cybersecurity threats are ever-evolving. Despite sustained and substantial investment in product security research and development, we remain committed to responding to customers' cybersecurity requests with an open and transparent attitude. EDAN will always strive to continuously strengthen the cybersecurity defense of medical devices in a dynamically changing security environment, and fully ensure the safety and reliability of our products in clinical use.