Information On How to Report Security Issues

Protecting our customers from threats to their security is always an important task for DNX(Delta Networks (Xiamen) Ltd.). As a key player in global Networking and Smart Home markets, we will do our utmost to provide our users with secure stable products and services, and to strictly protect the privacy and security of their data.
We welcome and encourage all reports related to product security or user privacy. We will follow established processes to address them and provide timely feedback.

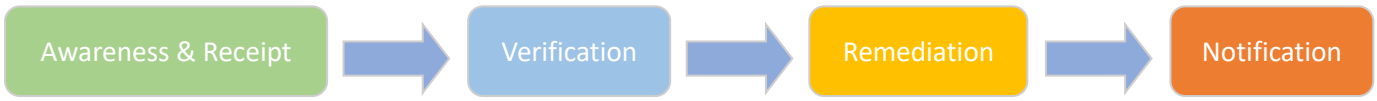
Report Vulnerabilities to DNX

We strongly encourage organizations and individuals to contact DNX's security team to report any potential security issue.
To report a security or privacy vulnerability, please send an email to **DPO@vidagrid.com** with the product model and software version, describe the detailed security issue to us. DNX will endeavor to respond to the report within 5 working days.
DNX will need to obtain detailed information about the reported vulnerability to more accurately and quickly begin the verification process.

Responsible Reporting Guidelines

1. All parties to a vulnerability disclosure should comply with the laws of their country or region.
2. Vulnerability reports should be based on the latest released firmware, and preferably written in English.
3. Adhere to data protection principles at all times and do not violate the privacy and data security of DNX's users, employees, agents, services or systems during the vulnerability discovery process.
4. Adhere to data protection principles at all times and do not violate the privacy and data security of DNX's users, employees, agents, services or systems during the vulnerability discovery process.
5. Maintain communication and cooperation during the disclosure process and avoid disclosing information about the vulnerability prior to the negotiated disclosure date.
6. DNX is not currently operating a vulnerability bounty program.

How DNX Deals with Vulnerabilities



DNX encourages customers, vendors, independent researchers, security organizations, etc. to proactively report any potential vulnerabilities to the security team. At the same time, DNX will proactively obtain information about vulnerabilities in DNX products from the community, vulnerability repositories and various security websites. In order to be aware of vulnerabilities as soon as they are discovered.
DNX will respond to vulnerability reports as soon as possible, usually within 5 business days.
DNX Security will work with the product team to perform a preliminary analysis and validation of the report to determine the validity, severity, and impact of the vulnerability. We may contact you if we need more information about the reported vulnerability.
Once the vulnerability has been identified, we will develop and implement a remediation plan to provide a solution for all affected customers.
Remediation typically takes up to 90 days and in some cases may take longer.
You may at any time stay updated on our progress and the completion of all remediation activities via the contact information specified in this policy.

DNX will issue a security advisory when one or more of the following conditions are met:

1. The severity of the vulnerability is rated CRITICAL by the DNX security team and DNX has completed the vulnerability response process and sufficient mitigation solutions are available to assist customers in eliminating all security risks.

2. If the vulnerability has been actively exploited and is likely to increase the security risk to DNX customers, or if the vulnerability is likely to increase public concern about the security of DNX products, DNX will expedite the release

of a security bulletin about the vulnerability, which may or may not include a full firmware patch or emergency fix.

Information on Minimum Security Update Periods

The Support Period for DNX components is actively maintained considering security updates from Jan 2025 to Jan 2030.

*This list is subject to change only to extend support periods or include additional models. No published defined support period will ever be shortened. Updates will be notified.

Models	Versions	Description
VCB-5106-WB	V1.0.0.0	Wi-Fi Dongle
VCB-5107-WB	V1.0.0.0	Wi-Fi Dongle
VD-600-WB	V1.0.0.0	Wi-Fi Dongle
VD-606-WB	V1.0.0.0	Wi-Fi Dongle
VD-606L7-WB	V1.0.0.0	Wi-Fi/LTE Dongle