Product Vulnerability Disclosure Policy

Expando welcomes independent security researchers, vendors, customers, and other stakeholders to responsibly report security vulnerabilities affecting our product portfolio.

Expando places a high priority on security concerns and is strongly committed to safeguarding our customers. Our goal is to timely analyze, validate, and provide corrective actions to address reported issues.

This policy outlines the procedure for reporting vulnerabilities to Expando, provides guidance to vulnerability reporters, and explains what you can expect once we receive your report. Expando reserves the right to deviate from this policy when necessary.

Reporting Product Vulnerabilities

If you need to report a potential security vulnerability in any Expando product, please send an email to support@expando.se.

All existing customers and suppliers should connect directly with their Expando contacts using the established support channels available to all customers.

When reporting a product security vulnerability, please include at least the following information to help us understand the scope and impact of the issue:

- Product and Product Version

- Detailed instructions on how to replicate the vulnerability

- Potential implications of the issue at hand

- Public disclosure plans

After receiving the report, our security team will send an acknowledgment to the reporter and begin the process of analyzing, validating, and taking corrective actions to address the vulnerability.

All information received in the report is considered confidential and will be shared only with the relevant stakeholders on a need-to-know basis.

For reporting security concerns in Expando's IT systems—for example, Expando's website or other non-product related issues, please use the same email address: support@expando.se.

Code of Conduct

By reporting and taking part in our vulnerability disclosure program, we expect the following from you:

• Perform only the minimum non-destructive actions necessary to obtain the proof of concept.

• Do not engage in any activities that could be damaging or disruptive to the availability or performance of the targeted systems.

• Do not violate any applicable laws or breach any agreements.

• To protect our customers, we request you refrain from publicly disclosing any vulnerabilities until we have addressed the issue.

• Please inform us as soon as possible if you have any plans for disclosure.

After validating the vulnerability, we will work to provide a resolution and collaborate with you, as needed, throughout the vulnerability investigation process.

The timelines to respond and address vulnerabilities depend on several factors such as the severity of the vulnerability, the scope and complexity of the issue, and the product life cycle.

If we discover or identify a vulnerability in products or code developed by other vendors, we will communicate the response to the reporter and support communication with the relevant vendor to the best of our knowledge.

External Communications

When a reported vulnerability is addressed and a solution is available, we will notify affected customers using the appropriate communication channels. The communication will include a description of the vulnerability and, if applicable, details of the affected products and versions along with guidance on how to address the issue.

Contact Information

If you have additional questions regarding this policy, please contact us by email at support@expando.se.