Vulnerability Disclosure Policy

Introduction

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link email: VIDAASecurity@vidaa.com. In your report please include:

· Model number on which the vulnerability can be observed

· Title of vulnerability (mandatory)

· Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations) (mandatory)

· Impact (what could an attacker do?) (mandatory)

· Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

· Contact Information. If you would like us to follow-up with you with status reports, please provide us with sufficient contact information, such as contact name and email address, so that we can keep in touch with you. You are not required to provide contact information to submit a report. Please note your contact information will only be used to contact you regarding the vulnerability you reported and will not be used for any other purpose. Your personal information will be protected as described in Privacy Policy (https://www.vidaa.com/privacy/).

What to expect

After you have submitted your report, and if you provide contact information, we will respond to your report within 7 calendar days to acknowledge the receipt of your report and aim to triage your report within 15 working days. We'll also keep you informed of our progress, including but not limited to:

· Status update of your report.

· Significant new information regarding to your report.

· Changes to existing fix plans.

· Disclosure plans, if any

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has

been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate with us.

Guidance

You must NOT:

· Break any applicable law or regulations.

· Access unnecessary, excessive or significant amounts of data.

· Modify data in the organization's systems or services.

· Use high-intensity invasive or destructive scanning tools to find vulnerabilities.

· Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.

· Disrupt the organization's services or systems.

Security Support Period

We take the growing risk of security threats to our products very seriously. We have long been committed to the ongoing effort to continuously provide security updates for our products. Device models will be supported with security updates for at least 4 years from their launch day which can be found below. We publish and update the End Of Life (EOL) device model list below on a periodic basis which includes the device models that are end of support and will not be maintained by any security updates, so you can check if your device is still supported. *Some device models may be supported with security updates for 5 years or even longer, depending on the actual situation. If a security vulnerability with extremely high risk is disclosed, we may still provide necessary security updates to you, even if your device is in the EOL product list.

Launch Date for Product

Product Launch Date

9618 2024/3/8

72690 2024/1/31