Responsible Disclosure policy

02/04/2024

AMARON B.V. (S.R.L.)
Kapellestraat 13
8755 Ruiselede
T +32 (0)51 62 73 20F +32 (0)51 43 33 81

TVA BE 0812.300.071
IBAN BE96 0017 0057 5405
BIC GEBABEBB

1 Table of contents

2 The purpose of this policy

Amaron aims to identify solutions to vulnerabilities as quickly as possible in line with the severity of the vulnerability. Amaron values parties that report vulnerabilities, provided they operate ethically and in accordance with the legal framework for ethical hacking.

With this document Amaron wants to provide a framework on how to deal correctly with ethical hackers.

3 How to report a security vulnerability?

Contact Amaron immediately via privacy@amaron.be no later than 72 hours after the vulnerability was discovered. We ask you to provide us with the following data to enable Amaron to conduct a comprehensive analysis and reproduce the vulnerability:

- Description of the vulnerability
  - Type of vulnerability
  - Configuration details
  - Operating systems
  - IP address or URL of the affected system
  - Detailed, step-by-step report, including dates and times, on how you discovered the vulnerability.
- Include screenshots so that we can better analyze the vulnerability. Ensure that any personal data is redacted or obscured from the screenshots.
- Your name, organization name, and contact information, including a phone number for further communication.

All the aforementioned data must be forwarded in a document protected by a complex password. The password should be provided to Amaron by calling us on +32 51 62 73 20.

We retain this data for an extended duration in the context of a possible dispute.

4 How to deal with a vulnerability?

It is important to always respect the GDPR rules [1].

In the event that the party gains access to data through the identified vulnerability, any processing of that data is strictly forbidden

It should be clear that activities like phishing, spamming, brute force attacks, DDoS, copying or deleting data, installing malware, or causing damage to the system or data are explicitly prohibited.

[1] Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

5 Cooperation

The objective is for both parties to collaboratively find a solution to prevent adverse consequences. The party discovering the vulnerability is therefore also obliged to assist Amaron free of charge. Amaron can provide a reward if substantial time is requested from the discovering party of the vulnerability. For authorized activities (e.g. penetration testing on behalf of Amaron), reimbursement will be in accordance with the agreement with the party.

6 Vulnerability Reporting and Publication

Only Amaron holds the authority to decide whether to disclose the vulnerability to its customers, Cyber Security Belgium, the data protection authority, the police, or other relevant parties. The party (e.g. an ethical hacker) discovering the vulnerability is not allowed to make this decision. Public disclosure of the vulnerability by the discovering party is strictly prohibited. It is essential to note that legal consequences may be incurred if:

- Hacking is conducted with malicious intent or results in damage.
- Hacking is performed with good intentions but not in accordance with the ethical hacking or GDPR laws.
- Non-compliance with the rules outlined in this policy occurs.

7 Disputes

This policy is subject to Belgian law. Disputes shall be brought before the courts/tribunals in the judicial district of West Flanders, Bruges division, which holds exclusive territorial jurisdiction.

8 Changes to this policy

We reserve the right to modify the content of this policy at any time, or to terminate the policy.