guardtime

DECEMBER 2020

Guardtime
Software and Service Vulnerability Policy

ID: GT/SW/VulnP
Version: 1.0
Effective from: 01 December 2019
Classification: Public
Review and maintenance: Head of Engineering
Approved by: CEO

Contents

1. Purpose and General Terms

A. This document is the Guardtime Software and Service Vulnerability Policy.

B. The purpose of this document is to provide top-level directives and a framework on how to address possible vulnerabilities in Guardtime products.

C. Guardtime has the right to amend this document at any time when justified and appropriate. New versions of this document are published at https://guardtime.com/library/general/ no later than 30 days before their enforcement.

2. References

Reference	Document
CVSS v3.1	Common Vulnerability Scoring System - Version 3.1
TLP v1.0	Traffic Light Protocol - Version 1.0

3. General Principles

A. Guardtime strives to help customers minimize the risk associated with vulnerabilities in Guardtime products.

B. Guardtime aims to provide customers with up-to-date information, guidance and mitigation options to address possible vulnerabilities.

C. Guardtime employs a rigorous process to continually evaluate and improve its vulnerability response practices.

D. Security patches to the products deployed are regularly reviewed and applied as appropriate.

E. Critical vulnerabilities are addressed within a period of 48 hours.

4. Reporting a Vulnerability

A. A security vulnerability identified in any Guardtime product should be reported immediately to security@guardtime.com. Timely identification of vulnerabilities is of high relevance in mitigating potential risks to Guardtime customers.

B. Guardtime security team will address the report and provide instructions for the next steps.

C. In case encryption of the communication is needed, the reporting party must contact the Guardtime security team to acquire a PGP key or agree on another suitable encryption mechanism.

D. When reporting a potential vulnerability, the reporting party should include as much of the following information as possible to help the Guardtime security team understand the nature and scope of the reported issue:

    a. Product name and version that contains the vulnerability.

    b. Environment or system information under which the issue was reproduced (e.g. OS version, etc.).

    c. Type and/or class of vulnerability (XSS, buffer overflow, RCE, etc.).

    d. Step-by-step instructions to reproduce the vulnerability.

    e. Proof-of-concept or exploit code.

    f. Potential impact of the vulnerability.

E. Any other security issues regarding Guardtime products should be reported also to security@guardtime.com.

5. Handling Vulnerability Reports

A. Guardtime appreciates any substantial feedback on the security and vulnerabilities of its products.

B. Guardtime believes in maintaining a good relationship with security researchers and acknowledges them in advisories (if desired). In return, researchers are asked to give an opportunity to remediate the vulnerability before publicly disclosing it. Guardtime believes that coordinating the public disclosure of a vulnerability is the key to protecting its customers.

C. All information about vulnerabilities disclosed according to this policy is intended to remain private between Guardtime and the reporting party (if the information is not already public knowledge) until a remedy is available and disclosure of activities are coordinated.

6. Vulnerability Remediation

A. After investigating and validating a reported vulnerability, Guardtime will develop and qualify the appropriate remedy for products that are under active support from Guardtime.

B. Guardtime makes every effort to provide the remedy or corrective action in the shortest commercially reasonable time.

7. Severity rating

A. A security vulnerability is classified by its severity rating, which is determined by many factors, including the level of effort required to

exploit a vulnerability as well as the potential impact to data or business activities from a successful exploit.

B. Guardtime uses the Common Vulnerability Scoring System version 3.1 (CVSS v3.1) to identify the severity level of identified vulnerabilities. The full standard, which is maintained by the Forum of Incident Response and Security Teams (FIRST), can be found at https://www.first.org/cvss.

C. If information disclosed contains TLP graduation, the TLP must be used when reporting about the security vulnerability. Guidelines on how to use TLP can be found at https://www.first.org/tlp/.

Appendix A: Document Versioning and Review History

A.1. Version History

Date (MM.YYYY)	Version	Author	Changes
05.2019	0.1	SOC	Document creation
10.2019	1.0		Final draft
11.2020	1.0		Yearly review, minor changes

A.2. Review Control

Reviewer	Section	Comments	Actions agreed
Head of Engineering			Next review in 12.2021