Certes Vulnerability Management and Disclosure Document

Certes Enforcement Points Software, CryptoFlow Net Creator Software and Certes Policy Manager Software

v1.0

Sept 2026

Table of Contents

List of Tables

List of Figures

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2026-04-13	Caleb Hughston	Initial draft.
1.0	2026-09-13	Matt Cable	Adding non-certified software and Final release

1. Introduction

This document defines how Certes Networks Inc., hereafter called Certes, manages vulnerabilities affecting the certified TOE after certification and, where applicable, vulnerabilities affecting other Certes software through the same internal vulnerability-management process.

It describes the steps for receiving vulnerability information, verifying and analyzing potential impact on certification compliance, developing and releasing remediation, and coordinating vulnerability disclosure with relevant stakeholders.

Certes develops and maintains the Certes Enforcement Points Software (CEP), CryptoFlow Net Creator Software (CFNC), and Certes Policy Manager Software (CPM). For purposes of this document, the certified TOE consists only of the specific product versions, configurations, and components identified in the applicable EUCC certificate and Security Target. Any other versions or configurations of CEP or CFNC, and CPM where it is outside the certified scope, are treated as non-certified software.

The TOE is distributed software running on multiple hardware models and virtual machines as network appliances that are high performance, low latency, bandwidth customizable, and provide network encryption. It provides data protection cryptography for layer 2 networks, and Internet Protocol (IP) packet encryption for layer 3 and layer 4 networks.

1.1 Purpose

The purpose of this document is to provide an auditable and repeatable vulnerability-management and disclosure procedure for the certified TOE and for non-certified software developed or maintained by Certes.

The EUCC-specific notification, impact-analysis, remediation, and disclosure requirements in this document apply to vulnerabilities affecting the certified TOE. Vulnerabilities affecting software outside the TOE are managed using the same underlying process but are approved and controlled internally unless the analysis identifies an actual or potential impact on the TOE, its certificate claims, certified configurations, or shared components.

1.2 Target Audience

The audience for this document consists of the Certes customers and Certes partners, Certes staff, the Certification Evaluation Laboratory staff, and the National Cybersecurity Certification Authority (NCCA).

2. Vulnerability Management Procedure

Certes applies this procedure to both certified and non-certified software. For the certified TOE, the procedure incorporates the EUCC vulnerability-management requirements and the applicable provisions of ISO/IEC 30111:2019. For non-certified software, the same process is used for internal assessment, remediation, approval, and record retention. EUCC-specific communication with the CB or NCCA is required when a vulnerability may affect the TOE or its certification.

2.1 Preparation

Certes maintains and publishes appropriate methods for receiving vulnerability information relating to its certified ICT products. These methods may also be used to report vulnerabilities in other Certes software, which will be handled under the internal process defined in this document.

Suspected vulnerabilities can be reported to Certes through publicly available contact methods. These include emailing **support@certesnetworks.com**, calling the Support Line from the USA at **+1 888-277-8395** or from outside the USA at **+1 412-262-2571 (option #2)**, or visiting the Certes customer support portal at http://support.certesnetworks.com.

Confirmed vulnerabilities affecting the certified TOE will be disclosed through the Certes customer support portal in accordance with the applicable EUCC, ISO/IEC 29147, and coordinated vulnerability-disclosure requirements. Reports concerning suspected or unconfirmed vulnerabilities, vulnerabilities affecting non-certified software, and exploitation details will not be made public unless disclosure is approved under the applicable disclosure process.

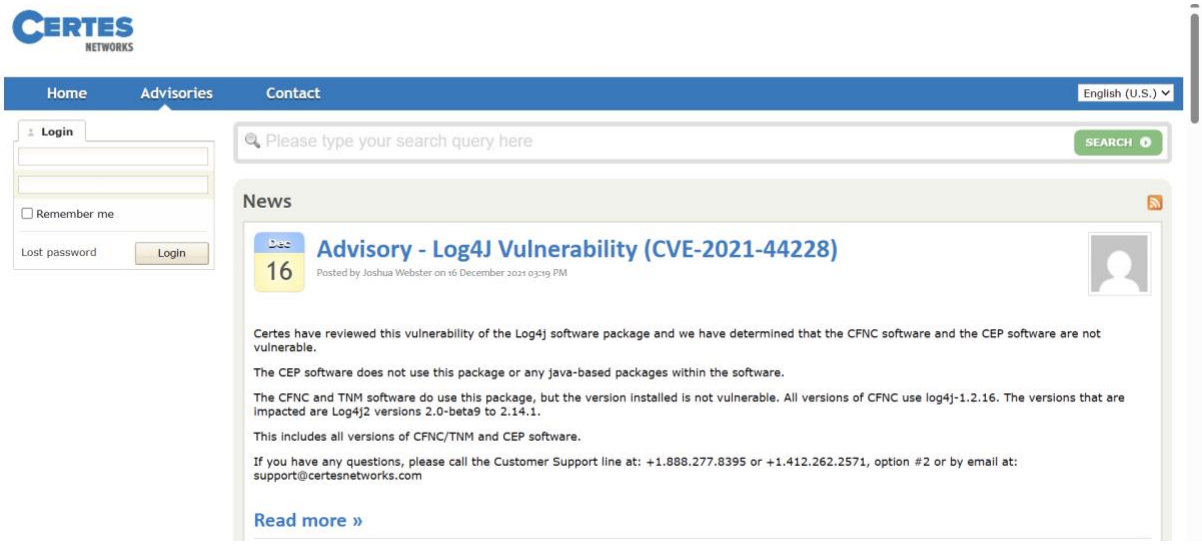

Figure 1- Certes customer support portal

2.2 Receipt

When Certes becomes aware of, or receives, information about a potential vulnerability affecting the TOE, the information shall be recorded, and a vulnerability impact analysis

shall be initiated. Vulnerabilities affecting non-certified software shall be recorded and assessed through the same process, with internal approval applied where no TOE impact is identified.

Information on potential vulnerabilities may be obtained through public contact channels, from the certification body, from publicly available repositories, or from other relevant sources. All records are retained for auditability and accountability purposes, including support for any supervisory activities.

Where the assessment concludes that a potential vulnerability affects only non-certified software and has no actual or potential impact on the TOE, the matter may be closed through Certes' internal approval process after the decision and its justification have been documented. Where the vulnerability affects the TOE, or its potential impact cannot be excluded, the EUCC-specific process shall continue.

To prevent repeated handling of unfounded or irrelevant notifications, Certes evaluates the reliability of information sources based on previous submissions and supporting evidence. Sources that are consistently assessed as unreliable may be documented and excluded from future consideration, with appropriate justification.

At receipt, the affected product or component shall be identified and classified as either within the certified TOE or outside the certified TOE. Where the affected software is initially classified as non-certified but may be shared with, integrated into, or otherwise affect the TOE, the matter shall be escalated for TOE impact analysis.

2.3 Verification

Following the recording of the information, Certes will carry out the vulnerability impact analysis, which includes verification activities and a more detailed technical assessment.

Verification shall determine whether the vulnerability affects the certified TOE, non-certified software only, or both. The analysis shall consider shared libraries, common source code, build outputs, deployment configurations, interfaces, dependencies, and security functionality used by the TOE.

The timeline is considered to start once Certes' preliminary assessment concludes that the vulnerability may have a potential impact on the conformity of the TOE within the scope of the certification.

In cases where a vulnerability is already being actively exploited and this information is publicly available, Certes will inform the CB without undue delay where applicable and support the implementation of appropriate measures, such as immediate remediation actions or the issuance of warnings.

Where a potential vulnerability may affect certification compliance, Certes will perform an attack potential calculation to assess whether the vulnerability is exploitable at the intended **AVA_VAN.3** level. Where permitted, any timeline extensions and mutual

agreements are managed and documented by Certes, and the NCCA will be informed as required.

The maximum timeframes for the vulnerability impact analysis are applied in line with **Table 1: Guidance on maximum timeframes for the vulnerability impact analysis** in [VMAD11].

Table 1- Certes maximum timeframes for the vulnerability impact analysis

Attack potential value range	Attacker potential category	Severity rating for remediation	Maximum timeframes
0–9	Basic	**Critical**	60 CD*
10–13	Enhanced-Basic	**High**	90 CD*
14–19	Moderate	**Medium**	Mutual Agreement
20–24	High	**Low**	Timing up to the certificate holder
≥25	Beyond High	**N.A.**	Timing up to the certificate holder

**CD = Calendar Days*

2.4 Impact Analysis Report

When exploitability is confirmed and the vulnerability applies to the TOE, an impact analysis report will be prepared and shared by Certes without undue delay with the CB or the NCCA, as applicable.
If the report contains exploitation details, the information is classified, for example using TLP, and handled with appropriate security measures to protect confidentiality, availability, and integrity and to ensure limited distribution where necessary.
If the report must be shared further, exploitation details are removed. All recipients will store the report and relevant documentation for at least five years.
A formal impact analysis report shall be prepared for vulnerabilities affecting the certified TOE or where the potential impact on the TOE cannot be excluded. For vulnerabilities confirmed to affect only non-certified software, Certes may use an internal vulnerability assessment record instead of submitting an impact analysis report to the CB, unless the CB reasonably requests relevant information.

2.5 Remediation Development

Where remediation is required, Certes will develop an appropriate remedial action and submit a proposal to the CB where the vulnerability affects the TOE or requires changes to the certified TOE. Since the TOE does not include an assessed patch management mechanism, the EUCC review process (EUCC Annex IV.3) for changes will be applied to verify correctness of changes and to reissue any necessary updated certificate.

For non-certified software, remediation shall be developed, reviewed, tested, and approved through Certes' internal change and release-approval process. Where the remediation also changes the TOE or affects a certified security function, the remediation shall be submitted to the CB in accordance with the EUCC requirements.

2.6 Release and Post-Release

Once remediation and associated changes are declared apt for deployment by the CB, Certes will proceed to deploy the remediation and associated changes, or release them in accordance with applicable supplementary cybersecurity information requirements. Remediation and associated changes will be implemented urgently and efficiently. Following release, the security lifecycle of the TOE will be updated as necessary to mitigate recurrence of the vulnerability or the relevant vulnerability class.

Remediation for non-certified software may be released following internal approval. If subsequent analysis shows that the remediation or the underlying vulnerability affects the TOE, the change shall be reclassified and handled through the applicable EUCC review and notification process.

3. Vulnerability Disclosure

Certes follows ISO/IEC 29147:2018 for general vulnerability disclosure. Once a strategy to correct a confirmed vulnerability is defined, or as soon as it is decided that the vulnerability cannot be mitigated, information related to a confirmed vulnerability affecting the certified TOE will be disclosed to the NCCA by the CB, including updates and progress of the strategy.
Information provided for NCCA purposes will not include exploitation details and will contain the necessary elements for the NCCA to understand the nature and impact on certification compliance, and the changes to be brought to the TOE. Information exchange between authorities will be performed securely and confidentially, including signed and encrypted communications.
Upon withdrawal of a certificate, Certes will disclose and register any publicly known and remediated vulnerability in the European vulnerability database or other online repositories.

4. References

This section describes the references to the documents used throughout the document.

Table 2 - Documentation References

Short Reference	Document Title
[CEM2022]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 2022 Revision 1.
[CC2022P1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model Version 2022, Revision 1.
[CC2022P2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components Version 2022, Revision 1.
[CC2022P3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components Version 2022, Revision 1.
[CC2022P4]	Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities Version 2022, Revision 1.
[CC2022P5]	Common Criteria for Information Technology Security Evaluation. Pre-defined packages of security requirements Version 2022, Revision 1.
[CCERR11]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1); Unique identifier: 002; Version: 1.1; Date of issue: 2024-07-22.
[CSA2019/881]	Regulation (EU) 2019/881 (Cybersecurity Act – CSA).
[CIR2024/3144]	Commission Implementing Regulation (EU) 2024/482 establishing the EUCC scheme, and Commission Implementing Regulation (EU) 2024/3144 amending it.
[D2022/2555]	Directive (EU) 2022/2555 (NIS 2 Directive).
[ISO/IEC 30111:2019]	ISO/IEC 30111:2019 (Vulnerability handling processes).
[ISO/IEC 29147:2018]	ISO/IEC 29147:2018 (Vulnerability disclosure).
[RFC 9116]	RFC 9116 (security.txt).
[VMAD11]	EUCC Scheme Guidelines on Vulnerability Management and Disclosure, Version 1.1, January 2025.

5. Acronyms and Terms

Table 3 defines the acronyms used throughout this document.

Table 3 – Acronyms and Terms

Acronym/Terms	Definition
CB	Certification Body
CC	Common Criteria
CEP	Certes Enforcement Point
Certified TOE	The software and configuration identified as the Target of Evaluation in the applicable EUCC certificate and Security Target
CFNC	CryptoFlow Net Creator
CPM	Certes Policy Manager
CSA	Certification Scheme Authority
EAL	Evaluation Assurance Level
EUCC	European Union Cybersecurity Certification
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NCCA	National Cybersecurity Certification Authority
Non-certified software	Certes software that is outside the scope of the applicable EUCC certificate.
TLP	Traffic Light Protocol
TOE	Target of Evaluation
TOE impact	An actual or potential effect on the TOE, its certified security functionality, certificate claims, certified configuration, or a shared component used by the TOE.