CERT.TG Description

RFC 2350

Version 1.0

1. About this document

This document contains a description of CERT.tg in accordance with RFC 2350. It provides basic information about CERT.tg, its channels of communication, and its roles and responsibilities.

1.1. Date of Last Update

This is version 1.0, published on 2020-12-07

1.2. Distribution List for Notifications

CERT.tg does not use any distribution lists to notify about changes in this document. This document is kept up-to-date at the location specified in 1.3.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available on the CERT.tg's website at: cert.tg/about-us/CERT-tg-RFC-2350-EN

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT.tg.
The PGP public key, ID and fingerprint are available in section 2.8 of this document.

Document Identification
Title: CERT-tg_RFC2350_EN
Version: 1.0
Document Date: 2020-12-07
SHA-256
Expiration: this document is valid until superseded by a later version

2. Contact Information

This section describes how to contact CERT.TG.

2.1. Name of the Team

CERT TOGO, National CERT of the Togolese Republic
Short Name: CERT.tg

2.2. Address

Ministère de l'Economie Numérique et de la Transformation Digitale
Avenue Abdoulaye Fadiga
07 BP 13215 - Lomé, Togolaise

2.3. Time Zone

UTC

2.4. Telephone Number

Phone: +228 22 53 59 80 / Mobile: +228 70 54 93 25

2.5. Facsimile Number

N/A

2.6. Other Telecommunication

N/A

2.7. Electronic Mail Address

For General Inquiries: contact@cert.tg
For information Security Incidents: incidents@cert.tg

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT.tg.
- Key ID: 0x2C5D9DBA
- Fingerprint: 48D0 0B2C 6163 8539 4C43 6927 8F35 B74A 2C5D 9DBA

The public PGP key is available on the following link and can be retrieved from one of the usual public key servers.

2.9. Team Members

The list of the CERT.tg's team members is not publicly available.
Information about the team members might be divulged upon request.

2.10. Other information

See our web site at www.cert.tg for additional information about CERT.TG

2.11. Points of Customer Contact

For general inquiries: contact@cert.tg
For information Security Incidents: incidents@cert.tg
We encourage our customers to use our cryptographic key to ensure integrity and confidentiality.

If it is not possible (or not advisable for security reasons) to use e-mail, CERT.tg can be reached by telephone
Phone: +228 22 53 59 80
Mobile: +228 70 54 93 25

CERT.tg's hours of operation are 7/7 24h all year long.

3. Charter

3.1. Mission Statement

CERT.tg is the national Computer Emergency Response Team (CERT) in Togolese Republic. Its mission is to identify, analyses and mitigate threats targeting the Togolese State, administrations, agencies and organizations of the State, citizens and Togolese companies.
CERT.tg contributes to ensuring cyber security of the Togolese nation.

3.2. Constituency

The primary constituency is composed of all Togolese Republic:

- All ministries, administrations and state services;
- Operators of Essential Services and Critical infrastructure operators as defined by the Togolese law;
- Other key players in sensitive sectors.
- All Citizens of the Togolese Republic

3.3. Sponsorship and /or Affiliation

Togolese Republic
Ministry of Digital Economy and Digital Transformation (MDEDT)
Ministry of Security and Civil Protection (MSCP)
Ministry of Economy and Finance (MEF)
National Cybersecurity Agency (NCA)
Regulatory Authority for Electronic Communications and Posts (RAECP)
Asseco Data Systems (ADS)

3.4. Authority

The establishment of the CERT.tg was mandated.
The "Decree 2019-098 portant création, attribution et organisation de la société CDA" defines competencies and authority of "CERT.tg".
CERT.tg is operated by Cyber Defense Africa (CDA) as a Service delegated by ANCy.
CDA operates under the authority of the MDEDT, MSCP and MEF.
ANCy operates under the authority of the Prime Minister (PM), MDEDT, MEF, Ministry of Armed Forces (MAF), Ministry of Justice (MJ) and Togolese Republic Presidency.

4. Policies

4.1. Types of Incidents and Level of Support

CERT.tg is authorized to address all types of computer and network security incidents, which occur, or threaten to occur, in Togolese Republic.

The level of support given by CERT.tg will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the availability of CERT.tg's resources at the time.

4.2. Co-operation, Interaction and Disclosure of Information

All information received by CERT.tg related to cyber security incidents is considered confidential and is used only to resolve incidents and prevent further incidents. Information that is sensitive (such as personal data, system configurations) or may be harmful, is processed in a secure environment and encrypted, if they must be transmitted over unsecured environment.

The information submitted to CERT.tg may be distributed to interested parties, such as other CERT teams, our technological partners, administrators of the affected resources, other entities included in the Togolese national cyber security system, on a need-to-know basis, for the sole purpose of incident handling (i.e., to the extent necessary to identify and mitigate the threat). No personally identifying information is exchanged, unless explicitly authorized.

Please visit our privacy statement on cert.tg/privacy-statement/

4.3. Communication and Authentication

The preferred method of communication is email.

1. For low sensitivity information, unencrypted methods such as emails or phones can be used.
2. All sensitive information shared to CERT.tg should be encrypted with our public PGP key detailed in Section 2.8.

5. Services

5.1. Incident Response

CERT.tg will provide incident response capabilities on a 24/7/365 basis in the following areas:

5.1.1. Incident triage

- Report assessment: Interpretation of incoming incident reports, prioritizing them, and relating them to ongoing incidents and trends.
- Verification: Help in determining whether an incident has really occurred, and its scope.

5.1.2. Incident Coordination

- Information categorization: Categorization of the incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- Coordination: Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.1.3. Incident Resolution

- Technical Assistance: This may include analysis of compromised systems.
- Eradication: Elimination of the cause of a security incident (the vulnerability exploited), and its effects.
- Recovery: Aid in restoring affected systems and services to their status before the security incident.

5.2. Proactive activities

5.2.1. Announcements

Announcements include intrusion alerts, vulnerability warnings and security advisories. Such announcements inform citizens and companies in CERT.tg constituency about new developments. Announcements enable receivers to protect their systems and networks against newly found problems before they can be exploited.

5.2.2. Technology Watch

CERT.tg monitors and observes new technical developments, intruder activities and related trends to help identify future threats.

5.2.3. Awareness

CERT.tg provides a comprehensive and easy-to-find collection of useful information that aids in improving security.

5.2.4. Education / Training

This service involves providing information to Togolese citizens, schools/universities and organizations about computer security issues through seminars, workshops, courses and tutorials.

5.2.5. Security Audits and assessments

CERT.tg provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards or ANCy.

5.2.6. Reporting

CERT.tg prepare and publish periodical reports about its operations and cybersecurity in Togo.

6. Incident Reporting forms

No specific form is needed to report security incidents via email or phone.
When reporting an incident on the CERT.tg website, some key information (contact, description of the incident, etc...) are mandatory. Please visit cert.tg/report-incident

7. Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, CERT.tg assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.