RFC2350 - CiviCERT

The Computer Incident Response Center for Civil Society

September 10, 2024

Contents

1 About this document **2**
- 1.1 Date of last update . . . 2
- 1.2 Distribution list for notifications . . . 2
- 1.3 Locations where this document may be found . . . 2
- 1.4 Authenticating this document . . . 2

2 Contact information **2**
- 2.1 Name of the team . . . 2
- 2.2 Postal Address . . . 2
- 2.3 Time zone . . . 2
- 2.4 Other telecommunications . . . 2
- 2.5 Electronic mail address . . . 2
- 2.6 Public keys and other encryption information . . . 3
- 2.7 Team members . . . 3
- 2.8 Other information . . . 3

3 Points of contact **3**

4 Charter **3**
- 4.1 Mission statement . . . 3
- 4.2 Constituency, Sponsorship and/or Affiliation . . . 4

5 Policies **4**
- 5.1 Types of incidents and level of support . . . 4
- 5.2 Co-operation, interaction and disclosure of information . . . 4
- 5.3 Communication and authentication . . . 5
- 5.4 Incident response . . . 5
  - 5.4.1 Incident triage . . . 5
  - 5.4.2 Incident coordination . . . 5
  - 5.4.3 Incident resolution . . . 5
- 5.5 Proactive services . . . 6

6 Incident reporting forms **6**

1 About this document

1.1 Date of last update

Version 1.1, published on 10th September 2024. the previous publicly published version was Version 0.93, published on 29th February 2016.

1.2 Distribution list for notifications

CiviCERT has a internal distribution list (rfc2350@civicert.org) to notify to its members about changes in this document.

1.3 Locations where this document may be found

The most updated version of this document is available at: https://www.civicert.org/rfc2350/

1.4 Authenticating this document

The PDF version of this document has been signed with the GPG key of civicert@civicert.org

Key fingerprint = 6352 E409 BF2D 87A7 8B38 C0A6 B67E 3CE2 78DE 520E

The signature is available from the following webpage: https://www.civicert.org/rfc2350/

2 Contact information

2.1 Name of the team

CiviCERT – Civil Society Computer Incident Response Center, the CERT for Civil Society.

2.2 Postal Address

CiviCERT is fiscally hosted by the Center for the Cultivation of Technology.

CiviCERT
c/o The Center for the Cultivation of Technology
Gottschedstr. 4
13357 Berlin
Germany

2.3 Time zone

Central European Time (UTC+0100, UTC+0200 from April to October)

2.4 Other telecommunications

We are exploring the possibilities to be available to receive messages via Signal, etc.

2.5 Electronic mail address

Incident reports related mail should be addressed to civicert@civicert org

2.6 Public keys and other encryption information

The public key of civicert@civicert org is available at: http://civicert.org/civicert_0x78DE520E.asc. the associated fingerprint is: 6352 E409 BF2D 87A7 8B38 C0A6 B67E 3CE2 78DE 520E

2.7 Team members

CiviCERT is an initiative of the Rapid Response Network (RaReNet) an umbrella organizations formed by the partnership between Internet Content and Service Providers, Non Governmental Organizations and individuals that contribute some of their time and resources to the community in order to globally improve the security awareness of civil society.

The core team (in alphabetical order by surname) is composed by the following members in their individual or organizational capacity:

Organization	Name	Email	Key fingerprint
Qurium	Anthony Briand	anthony.briand@virtualroad.org	EAA0 FB07 1528 C67A 8945 3ED9 FECC CD78 F0B7 1628
CiviCERT	Michael Carbone	michael@civicert.org	DACB 41C0 67AD 55D7 794B FB8D 6564 410F 1547 05F0
Digital Defenders Partnership	Alexandra Haché	alexandra@digitaldefenders.org	26B8 0B68 4304 B32E 5C9F C44B 04BC 4A57 85C9 3BF5
Qurium	Tord Lundstrom	t@virtualroad.org	9FDD 375A B71F 5633 F67E 2470 B2F7 1E95 E74D 4E02
Access Now	Beatrice Martini	beatrice@accessnow.org	F94F 205E A3E4 6979 E719 8D16 0C5F 23FF 7D5B 5AEC

2.8 Other information

Any other information about CiviCERT can be found at https://civicert.org and on the websites of each CiviCERT member.

3 Points of contact

The preferred method for contacting CiviCERT is via email: civicert@civicert.org. We encourage our beneficiaries to use GPG/PGP encryption when communicating with us.

As an alternative to encrypted email, CiviCERT provides a secure form to reach the support team. The form is available at: https://civicert.org/contact

If required, CiviCERT will establish an alternative secure channel of communication that might include encrypted messaging, encrypted voice call, or HTTPS-based web chat.

4 Charter

4.1 Mission statement

Established the 1st of January 2014, The main goal of CiviCERT is to improve the incident response capabilities of NGOs, journalists and involved citizens all around the world.

CiviCERT aims to close the gap and increase cooperation between civil society, activists on the one side and organizations or individuals working in information security on the other side. The members of the initiative are a mix between Internet providers' anti abuse teams, NGO project officers and citizens sensitized in freedom of speech and information security. CiviCERT's members donate time and resources to this community in order to globally improve the security awareness of civil society.

CiviCERT serves as secure proxy to report incidents they have been made aware of and provide information of best practices while protecting its beneficiaries and sources.

CiviCERT wants to build bridges with other computer emergency response teams (CSIRTs) and security communities by learning from the best practitioners in the security response field and helping other teams to understand the very specific environment that CiviCERT beneficiaries work.

4.2 Constituency, Sponsorship and/or Affiliation

CiviCERT operates thanks to the contributions of its members. Members of CiviCERT contribute skills and other assets into this initiative. When necessary CiviCERT will fund raise to obtain specific access to tools and technologies not available via its members.

CiviCERT is committed to always inform its beneficiaries of which sources of funding might enable or support any support activities.

During 2014-2016, CiviCERT's coordinating role was assumed by Qurium, a not-for-profit organization based in Sweden.

5 Policies

5.1 Types of incidents and level of support

CiviCERT works with all types of computer security incidents which occur, or threaten to occur, in the constituency networks (i.e. the ASN operated by its core members).

When a requests is related to an Internet resource does is not directly owned by its core members, CiviCERT will act as a expert advisor of its beneficiaries that operate such resource. Such expert role is regulated under a set of **confidentiality agreements** that guarantees that the beneficiary has the ultimate say about how all information including any personal data is handled in the event.

The level of support provided by CiviCERT will vary depending on the type and severity of the incident, the type of constituent or the size of the user community affected. CiviCERT is committed to response within two working days at maximum.

Incidents will be prioritized according to the **incident response roadmap** approved by the CiviCERT core members.

5.2 Co-operation, interaction and disclosure of information

Once an "event handling disclosure agreement" is reached with the beneficiary, CiviCERT will exchange all necessary information with other CSIRTs as well as with affected parties. Special attention will be taken to the handling of personal identifiable information and sensitive metadata. Neither personal nor overhead data are exchanged unless explicitly authorized.

All sensible data (such as personal data, geo location, system configurations, known vulnerabilities) will be always encrypted when transmitted over unsecured environment.

5.3 Communication and authentication

In view of the types of information that CiviCERT deals with, plain telephone or unencrypted mail will not be considered sufficiently secure. Secure communication channels with the beneficiaries and/or reporters is consider a mandatory pre-requirement for any event handling. While GPG encrypted email is the default recommended channel for information exchange, alternatives for those concern with the use of encryption are available.

CiviCERT relies heavily in its human network of practitioners on the field and authentication of information and sources relies in trusted referrers or proxies.

From the official point of view only data signed by CiviCERT generic GPG/PGP key or any other keys with the domain civicert.org included in this document can be attributed to CiviCERT.

5.4 Incident response

CiviCERT will assist NGOs or other forms of civil society organizations in handling the technical and organizational aspects of incidents in connection with other CSIRTs. In particular, CiviCERT will provide assistance or advice with respect to the following aspects of incidents management:

5.4.1 Incident triage

- Establish a secure communication channel with the reporter.
- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.
- Help gathering any extra forensic information needed.
- Identifying the best partner or skill set needed to address the incident.

5.4.2 Incident coordination

- Determining the initial cause of the incident.
- Facilitating contact with other organizations that which may be involved/affected.
- Providing human readable information for the victims to campaign if needed.
- Composing announcements to civil society if applicable.

5.4.3 Incident resolution

- Helping to remove the vulnerability.
- Helping to secure the system from the effects of the incident.
- Identify if the attack is targeted.
- Monitor the persistence of the attackers.
- Collecting evidence of the incident.

In addition, CiviCERT will collect statistics concerning incidents processed, and will notify the wider community as necessary to assist it in protecting against known attacks.

5.5 Proactive services

CiviCERT coordinates and maintains the following services to the extent possible depending on its resources:

- Security training for civil society
- Malware analysis
- Digital First Aid Kit https://gitlab.com/rarenet/dfak_2020
- Detection and packet analysis of network interference
- Legal advice
- Information sharing including MISP (Malware Information Sharing Platform)

6 Incident reporting forms

CiviCERT has created an encrypted web form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out. The form is available at: https://www.civicert.org/report-incident/