CARICERT Profile

Established according to RFC 2350

Version: 1.0

1. Document Information

1.1. Date of Last Update

This is version 3 of 13 May 2013.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 .

E-mail notification of updates will be sent to:

- All CARICERT members and employees of the Curaçao Bureau Telecommunication and Post (BT&P)
- All registered CARICERT constituents
- Any such parties with which CARICERT has an explicitly defined working relationship
- The FIRST (worldwide), LACNIC (South America) and Trusted Introducer (Europe) CSIRT communities

Any questions about updates please address to the CARICERT e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on http://www.caricert.cw/contactus.php .

2. Contact Information

2.1. Name of the Team

Full name: CARICERT

Short name: CARICERT

CARICERT is the national CERT or CSIRT of Curaçao.

2.2. Address

Bureau Telecommunication and Post

CARICERT

Beatrixlaan 9

Curaçao

2.3. Time Zone

GMT/UTC-4 (No DST)

2.4. Telephone Number

+5999 4631700

2.5. Facsimile Number

+5999 7364157

Note: this is not a secure fax, but it is situated within the secure CARICERT premises.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

cert@caricert.cw

This address can be used to report all security incidents to which relate to the CARICERT constituency,

2.8. Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication. CARICERT provides all CARICERT team members with keys, to be used for signing and encryption.
For general use, CARICERT has 2 keys which are replaced annually (2013 is the current year):

- CARICERT 2013 ** Encryption Only ** Key cert@caricert.cw : please use this key when you want/need to encrypt messages that you send to CARICERT (please sign your messages using your own key - it really helps when that key can be found on the public keyservers)

- CARICERT 2013 ** Signing Only ** Key : when due, CARICERT will sign messages using this key.

The current CARICERT team-keys can both be found on http://www.caricert.cw/contactus.php and are also present on the public keyservers (e.g. https://pgp.surfnet.nl).

2.9. Team Members

No information about the CARICERT team members is provided in public.

2.10. Other Information

- See the CARICERT webpages http://www.caricert.cw **.**
- CARICERT has applied for FIRST membership and Accreditation by the Trusted Introducer.

2.11. Points of Customer Contact

- Regular cases: use CARICERT e-mail address.
- Regular response hours: Monday-Friday, 08:00-17:00 (except public holidays in Curaçao).
- EMERGENCY cases: send e-mail to cert@caricert.cw with **URGENT** in the subject line.

3. Charter

3.1. Mission statement

The mission of CARICERT is to co-ordinate the resolution of IT security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring by means of announcements, alerts, warnings and advice.

3.2. Constituency

CARICERT is the national CERT or CSIRT of Curaçao. Therefore the country of Curaçao is the main constituency.

Priorities lie with the following sectors:

- Telecom / IT
- Finance
- Utilities (Energy, water, airport, etcetera)
- Government

CARICERT is set-up to deliver services to their registered constituents. Registration can also be on contract basis for specific services and as such is open to similar sectors in the Caribbean area outside Curaçao.

The constituency includes:

- *.an (old Netherlands Antilles tld – is being phased out) as far as based on Curaçao
- *.cw (new Curaçao tld)
- all computer systems and IP-addressable devices situated on Curaçao
- any other systems/networks belonging to other registered constituents

3.3. Sponsorship and/or Affiliation

CARICERT is part of the Curaçao Bureau Telecommunication and Post (BT&P).

3.4. Authority

The team coordinates security incidents on behalf of the country of Curaçao and of their registered constituents - and has no authority reaching further than that. The team is however expected to make tactical and operational recommendations in the course of their work. Such recommendations can include but are not limited to (temporarily) blocking or filtering addresses or networks. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled **URGENT**, in which case they are high priority. CARICERT itself is the authority that can set high priority back to normal – and the other way around. An incident can be reported to CARICERT as **URGENT**, but it is up to CARICERT to decide whether or not to uphold the high priority status.

4.2. Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled securely by CARICERT, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly by using the label "**CONFIDENTIAL"** in the subject field of e-mail. We recommend using e-mail encryption.

CARICERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CARICERT will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymised fashion.

If you object to this default behavior of CARICERT, please make explicit what CARICERT can do with the information you provide. CARICERT will adhere to your policy, but will also point out to you if that means that CARICERT cannot act on the information provided.

CARICERT does not report incidents to law enforcement, unless national law requires so. Likewise, CARICERT only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that CARICERT cooperates in an investigation. When a court order is absent, CARICERT will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP/GnuPG in all cases where highly sensitive information is involved is highly recommended.

In cases where there is doubt about the authenticity of information or its source, CARICERT reserves the right to authenticate this by any (legal) means.

5. services

5.1. Incident Response (Triage, Coordination and Resolution)

CARICERT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). CARICERT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however CARICERT will offer support and advice on request.

5.2. Proactive Activities

CARICERT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking, and also of ongoing attacks/threats when known/reported to CARICERT.

This role is one of advice only: CARICERT is not responsible for implementation.

6. Incident Reporting Forms

Not available. Preferably report in plain text using e-mail - or use the phone.

7. Disclaimers

None.