FORTHcert Profile
according to RFC 2350

Accredited by TRUSTED Introducer The European CSIRT Directory

1. About this document

1.1 Date of Last Update

This is version 1, published 2012/02/1.

1.2 Distribution List for Notifications

The latest version of this profile can be found on the location specified in 1.3

1.3 Locations where this Document May Be Found

The current version of this document is available from the FORTHcert web site at: http://www.forth.gr/forthcert/rfc2350.pdf

2. Contact Information

2.1 Name of the Team

"FORTHcert" is the Foundation for Research and Technology – Hellas, Computer Emergency Response Team.

2.2 Address

FORTHcert
FORTH - ICS
N. Plastira 100
Vassilika Vouton
Heraklion, Crete
GR 711 10 Greece

2.3 Time Zone

Eastern European Time EET (UTC+2, and UTC+3 from April to October)

2.4 Telephone Number

+30 2810 391-640

2.5 Facsimile Number

+30 2810 391-641 (this is *not* a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

cert@forth.gr

2.8 Public Keys and Other Encryption Information

FORTHcert has a PGP key, with
KeyID is 0x9A193C55
Fingerprint is F59D 140A 6C18 22E9 011D 0E2F E279 5570 9A19 3C55

The current PGP team key can be found at:
http://www.forth.gr/forthcert/contact-info.html

2.9 Team Members

Management, liaison and supervision are provided by Ioannis Askoxylakis
Head of FORTHcert

Team members, along with their contact information and public PGP keys, are listed in the FORTHcert web pages, at
http://www.forth.gr/forthcert/contact-info.html

2.10 Other Information

General information about FORTHcert, as well as links to various recommended security resources, can be found at
http://www.forth.gr/forthcert/index.html

FORTHcert is accretited by the Trusted Introducer for CERTs in Europe, more information at
https://www.trusted-introducer.org/teams/forth-cert.html

FORTHcert is a full member of FIRST, more information at
http://www.first.org/members/teams/forthcert

2.11 Points of Customer Contact

The preferred method for contacting FORTHcert is via e-mail at:
cert@forth.gr

If it is not possible (or not advisable for security reasons)
to use e-mail, FORTHcert can be reached by telephone during

regular office hours.

FORTHcert hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except Greek holidays).

If possible, when submitting your report, use the form mentioned in section 6.

3. Charter

3.1 Mission Statement

FORTHcert is the Incident Response Team of the Foundation for Research and Technology - Hellas. FORTHcert operates under the Institute of Computer Science and provides services relating to information security incidents. Its mission is to perform security incident coordination services for its members, to disseminate information regarding information security issues, to provide a national point of contact to international security community and to promote education and training.

3.2 Constituency

FORTHcert's constituency is the FORTH community. FORTHcert may provide CERT support to other public or private organizations upon signing a binding legal agreement.

3.3 Sponsorship and/or Affiliation

FORTHcert is a department of the Foundation of Research and Technology – Hellas, Institute of Compuer Science.

3.4 Authority

FORTHcert coordinates incidents on behalf of its constituency. FORTHcert is authorized to take operational actions regarding vulnerabilities and mitigation of incidents. Such actions may include but are not limited to blocking access to the FORTH network.

4. Policies

4.1 Types of Incidents and Level of Support

FORTHcert is authorized to address all types of computer security incidents which occur, or threaten to occur, at FORTH.

FORTHcert will respond to request for assistance by other CERTs external to FORTH.

FORTHcert will usually respond within the same work day to request for incident response.

4.2 Co-operation, Interaction and Disclosure of Information

FORTHcert wishes to acknowledge the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites, FORTHcert will otherwise share information freely in order to assist with the resolution and/or prevention of security incidents.

FORTHcert may release information to any third party or to governing authorities whenever there is a legal obligation to do so. However, FORTHcert may in some cases delay this action until such it has been established irrevocably, e.g. by court order. FORTHcert will in such cases always notify the affected persons or organisations. Information being considered for release will be handled as follows:

Private information is information about particular users, or applications, which must be considered confidential for legal, contractual, and/or ethical reasons. Private information will be released outside FORTHcert after all identifying parts have been removed "

Intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record). However it will be exchanged freely with system administrators and CSIRT's tracking an incident.

Private site information will not be released without the permission of the site in question.

Vulnerability information will be released freely, though every effort will be made to inform and work with the relevant vendor before the general public is informed.

Statistical information will be released at the discretion of FORTHcert.

Other sites and CSIRT's, when they are partners in the investigation of a computer security incident, can be trusted with confidential information. This will happen only if the other site's credentials can be verified and the information transmitted will be limited to that which is likely to be helpful in resolving the incident.

Law enforcement officers will receive legally required cooperation from FORTHcert.

4.3 Communication and Authentication

The preferred method of communication is by digitally signed email by using either PGP (see section 2.8 above) or other well known cryptographical means. Note digital signatures with self signed certificates will not be considered secure.

Telephone communication will be considered sufficiently secure to be used even unencrypted.

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of non-sensitive data.

Where it is necessary to establish trust, for example before relying on information given to FORTHcert, or before disclosing confidential information, the identity and trust level of the other party will be ascertained to a reasonable degree. Within the constituency, and referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST or TI members, the use of WHOIS and other Internet registration information, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures. Note that self signed digital certificates are not considered adequate for establishing the identity of the communicating party.

5. Services

5.1 Incident Response

FORTHcert is responsible for the coordination of response to security incidents. FORTHcert will work together with the Department of Systems and Networks (system administrators) at FORTH in handling the technical and organizational aspects of incidents.

5.1.1 Incident Triage

- Investigating the validity of the incident
- Determining the operational impact of the incident.
- Assigning a priority for incident response

5.1.2 Incident Coordination

- Document the incident.
- Coordinate contact with other sites which may be involved.
- Coordinate contact FORTH Management, Legal Office and/or appropriate law enforcement officials, if necessary.

- Provide information reports to other CERTs.
- Provide announcements to users, if applicable.

6. Incident Report Forms

An incident can be reported via form submission at
http://www.forth.gr/forthcert/report-online.php

7. Disclaimers

While care will be exercised in the preparation of information, notifications and alerts FORTHcert assumes no responsibility for errors or omissions or for damages resulting from the use of the information contained within.