CERT Intrinsec

RFC 2350

April 2019

INTRINSEC

Innovative by design

Website
www.intrinsec.com

Blog
securite.intrinsec.com

Twitter
@Intrinsec

Tour CBX 1, Passerelle des Reflets - 92400 Courbevoie France • TEL +33 1 41 91 77 77 • FAX +33 1 41 91 77 78
INTRINSEC SECURITE • SIREN : 812 535 284 • APE : 6203Z

TABLE OF CONTENT

1 1. Document Information

This document contains a description of CERT-Intrinsec in according to RFC 2350.

It provides basic information about the CERT-Intrinsec team, its channels of communication, its roles and responsibilities.

It also describes its responsibilities and the services offered.

1.1 Date of Last Update

Version 1.0, created on 2018-01-11.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document may be Found

The current and latest version of this document is available from CERT-Intrinsec's website. Its URL is:

https://www.intrinsec.com/wp-content/uploads/2019/01/CERT-Intrinsec-RFC2350.pdf

1.4 Authenticating this Document

This document has been signed with the CERT-Intrinsec's PGP key. The signature is available from CERT-Intrinsec's website. Its URL is:

https://www.intrinsec.com/wp-content/uploads/2019/01/CERT-Intrinsec-RFC2350.pdf.sig

1.5 Document Identification

Title: "CERT-Intrinsec RFC-2350"

Version: 1.0

Document Date: 2019-04-29

Expiration: this document is valid until superseded by a later version.

2 Contact Information

This section describes how to contact CERT-Intrinsec.

2.1 Name of the Team

CERT-Intrinsec

CERT-Intrinsec is Intrinsec's commercial and internal CERT.

2.2 Address

CERT-Intrinsec

La Défense - Tour CBX

1, Passerelle des Reflets - 92400 Courbevoie

France

2.3 Time Zone

CET / CEST

2.4 Telephone Number

+33 (0)1 47 28 38 39

2.5 Facsimile Number

None available.

2.6 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving your company or Intrinsec, please contact us at **cert@intrinsec.com**.

2.7 Public Keys and Encryption Information

CERT Intrinsec has a PGP key :

ID : 0x67823b64e8afd0d5

Fingerprint : 15F329628D03DBF6DC4D409067823B64E8AFD0D5

The key can be retrieved from one of the usual public key servers such http://pgp.mit.edu/

This key shall be used whenever information must be sent to CERT-Intrinsec in a secure manner.

2.8 Team Members

CERT-Intrinsec's team leader is Kilian LAVIEILLE.

The team consists of Intrinsec's IT security analysts.

2.9 Other Information

General information regarding CERT-Intrinsec can be found at the following URL:

https://www.intrinsec.com/cert-intrinsec/
https://securite.intrinsec.com/cert-intrinsec/

CERT-Intrinsec is listed by the Trusted Introducer for CERTs in Europe, see:

https://www.trusted-introducer.org/directory/teams/cert-intrinsec.html

2.10 Points of Customer Contact

The preferred method to contact CERT-Intrinsec team is to send an email to the cert@intrinsec.com address, which is monitored during hours of operation.

Urgent cases can be reported by phone during regular office hours on +33 (0)1 47 28 38 39.

CERT-Intrinsec's hours of operation are usually restricted to regular French business hours (Monday to Friday 09:30 to 18:00).
Out of office hours operations in case of emergency.

3 CHARTER

3.1 MISSION STATEMENT

CERT-Intrinsec is a private CERT team delivering Security services, mainly in France and Europe.
CERT-Intrinsec is also in charge of incident handling for Intrinsec.

Its purpose is two-folded:

- First, to assist its customer community in implementing proactive measures to reduce the risks of computer security incidents.
- And second, to assist its customer community in responding to such incidents whenever they occur.

CERT-Intrinsec's mission is to support its customer community to protect themselves against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests.
The scope of CERT-Intrinsec's activities cover prevention, detection, response and recovery.
CERT-Intrinsec is in charge of digital forensics and incident response (DFIR) activities.

CERT-Intrinsec will operate according to the following key values:

- CERT-Intrinsec strives to act according to the highest standards of ethics, integrity, honesty and professionalism.
- CERT-Intrinsec is committed to deliver a high-quality service to its constituency.
- CERT-Intrinsec will ensure to respond to security incidents as efficiently as possible.
- CERT-Intrinsec will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

3.2 CONSTITUENCY

CERT-Intrinsec primary constituency is composed of all the elements of Intrinsec's Information System: its users, its systems, its applications and its networks.

However, notwithstanding the above, CERT-Intrinsec's services are also delivered to a secondary constituency.
As a commercial CERT, the CERT-Intrinsec also provides services to its Customers Community, who subscribed a Service Level Agreement support contract.

3.3 Sponsorship and/or Affiliation

CERT-Intrinsec is part of Intrinsec: https://www.intrinsec.com/.

CERT-Intrinsec maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis.

3.4 Authority

For internal matters, CERT-Intrinsec operates under the authority of the CEO of Intrinsec.

For external incidents, CERT-Intrinsec coordinates security incidents on behalf of its constituency, and only at its constituents' request.

4 POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERT-Intrinsec addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see 3.2).

The level of support given by CERT-Intrinsec will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CERT-Intrinsec's resources at the time. Depending on the security incident's type, CERT-Intrinsec will gradually roll out its services which include incident response and digital forensics.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT-Intrinsec considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT-Intrinsec's constituency.

Consequently, CERT-Intrinsec exchanges all necessary information with affected parties, as well as with other CSIRTs, CERTs, SOCs, on a need-to-know basis. However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CERT-Intrinsec will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymised way only (unless other contractual agreements apply).

All incoming information is handled confidentially by CERT-Intrinsec, regardless of its priority. All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environment as stated below.

CERT-Intrinsec supports the Information Sharing Traffic Light Protocol version 1.1 (ISTLP, see https://www.trusted-introducer.org/ISTLPv11.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT-Intrinsec operates within the current French legal framework.

4.3 COMMUNICATION AND AUTHENTICATION

CERT-Intrinsec protects sensitive information in accordance with relevant regulations and policies within France and the EU.

CERT-Intrinsec respects the sensitivity markings allocated by originators of information communicated to CERT-Intrinsec (“originator control”).

CERT-Intrinsec also recognises and supports the ISTLP version 1.1.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

5 SERVICES

5.1 ANNOUNCEMENTS

CERT-Intrinsec provides information on the threat landscape, published vulnerabilities, new attack tools or artifacts and security measures needed to protect its constituency's Information System.

5.2 ALERTS AND WARNINGS

CERT-Intrinsec disseminates information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency.

Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

5.3 PRE-EMPTIVE SECURITY CONTROLS

CERT-Intrinsec performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.

5.4 DIGITAL FORENSICS AND INCIDENT RESPONSE (TRIAGE, COORDINATION AND RESOLUTION)

CERT-Intrinsec performs incident response for its constituency (as defined in 3.2).

CERT-Intrinsec handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency.
However, CERT-Intrinsec will offer support and advice on request.

CERT-Intrinsec will assist IT Security team in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

- Incident Triage:
  - Investigating whether indeed an incident occured.
  - Determining the extent of the incident.
- Incident Coordination:

- Determining the initial cause of the incident (vulnerability exploited).
- Performing data acquisition and analysis (hard drive and memory forensics)
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary and if requested by our constituency.
- Making reports to other CSIRTs, CERTs, SOCs.
- Composing announcements to users, if applicable.

- Incident Resolution:
  - Providing support for removing the vulnerability.
  - Providing support for securing the system from the effects of the incident.
  - Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
  - Collecting evidence where criminal prosecution, or University disciplinary action, is contemplated.

5.5 Development of Security Tools

CERT-Intrinsec internally develops security tools for its own use or use of his constituency. Some of them are also shared on Intrinsec's Github account : https://github.com/Intrinsec/

6 INCIDENT REPORTING FORMS

No local form has been developed to report incidents to CERT-Intrinsec.

If possible, please provide the following information:

- Contact information, including electronic mail address and telephone number
- Date and time when the incident started
- Date and time when the incident was detected
- Incident description
- Affected assets, impact
- Actions taken so far

7 DISCLAIMERS

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