RFC2350
VINCI-CERT

Author Vincent Le Toux (Head of VINCI-CERT)
Validated by Benoît Herment (Group CISO)
Version 2021-12-02

About this document

This document contains a description of VINCI-CERT according to RFC 2350. It provides information about the CERT, how to contact the team, and describes its responsibilities and the services offered by VINCI-CERT.

Distribution List for Notifications

There is no distribution list for notifications.

Locations where this Document May Be Found

The current version of this document can be found at: https://www.vinci.com/cert/vinci-cert.nsf/bib/files/$file/RFC2350-VINCI-v2.pdf

Contact Information

Name of the Team

"VINCI-CERT": the VINCI Computer Emergency Response Team Coordination Center.

Address

VINCI-CERT
1973, Boulevard de la Défense
92000 Nanterre, France

Time Zone

CET / CEST – Paris Time

Telephone Number

None available.

Facsimile Number

None available.

Other Telecommunication

None available.

Electronic Mail Address

cert@vinci.com

Public Keys and Other Encryption Information

Our current PGP-Key may be obtained by sending a request by mail for that at cert@vinci.com

Team Members

The Team leader is Vincent LE TOUX. The team consists of IT security analysts.

Other Information

The VINCI-CERT Portal is available at: https://www.vinci.com/cert

Points of Customer Contact

VINCI-CERT prefers to receive incident reports via e-mail. Please use our cryptographic keys above to ensure integrity and confidentiality.

VINCI-CERT 's hours of operation are restricted to regular business hours (09:00-18:00 Monday to Friday), all year long.

Charter

Mission Statement

VINCI-CERT's mission is to coordinate and investigate IT security incident response for the French Group: VINCI.

The VINCI-CERT will investigate any security incident that may involve the VINCI group entity as a source or target of an attack or any cyber-threat.

Constituency

Our constituency are composed of VINCI Group and all subsidiaries.

For a complete list and more information please see http://www.vinci.com

Sponsorship and/or Affiliation

VINCI-CERT is the Computer Security Incident Response Team (CSIRT) for the VINCI Group.

Funding is provided by the VINCI group.

VINCI-CERT operates under the authority of the management of the VINCI group.

Policies

Types of Incidents and Level of Support

VINCI-CERT addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident, the number of affected entities within our constituency, and our resources at the time.

Usually, our first response comes on the same working day during working hours, if not it will be on the following working day.

Co-operation, Interaction and Disclosure of Information

VINCI-CERT will exchange all necessary information with other CSIRTs as well as with other affected parties if they are involved in the incident or incident response process.

No incident or vulnerability related information will be given to other persons. French law enforcement personnel requesting information during a criminal investigation will be given the requested information within the limits of the court order and the criminal investigation, if they present a valid court order from a French court.

Communication and Authentication

All e-mails sent to the VINCI-CERT should be signed using PGP. All e-mails containing confidential information should be encrypted and signed using PGP. Information received in encrypted form should not be stored permanently in unencrypted form.

For other communication, a phone call, postal service, or unencrypted e-mail may be used.

VINCI-CERT supports the Information Sharing Traffic Light Protocol (TLP).

Services

Incident Response

The team offers the following services:
- Incident analysis

- Incident response support
- Incident response coordination
- Vulnerability response coordination

Proactive Activities

The team offers the following services:
- Intrusion detection services
- Auditing services

Incident Reporting Forms

We do not have an incident reporting form. Please report security incidents via encrypted e-mail to cert@vinci.com.
Incident reports should contain the following information:
- Incident date and time (including time zone)
- Source IPs, ports, and protocols
- Destination IPs, ports, and protocols
- And any relevant information

Disclaimers

This document is provided 'as is' without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

If you notice any mistakes within this document, please send a message to us by e-mail. We will try to resolve such issues as soon as possible.