SYNACKTIV

CSIRT Synacktiv

Information

version 1.2 (2022-10-25)

RFC 2350

TLP:WHITE

Information may be distributed without restriction

Twitter Linkedin Github

www.synacktiv.com 5, boulevard Montmartre – 75002 Paris Tel : 0033 1 45 79 74 75

1. Document Information

This document follows the RFC2350 specification (https://www.ietf.org/rfc/rfc2350.txt)

1.1. Date of last update

Version 1.0, published the 28th september 2021

1.2. Distribution list for notifications

Notifications of updates are submitted if you asked to be registered (csirt@synacktiv.com). The subject must be "registration to notification" and the body the purpose of your request.

1.3. Location where this document may be found

https://www.synacktiv.com/sites/default/files/2022-10/rfc2350-csirt_synacktiv-en-1.2.pdf

1.4. Authenticating this document

The signature of this document is available on the CSIRT Synacktiv website.

2. Contact Informations

2.1. Name of the Team

CSIRT Synacktiv

2.2. Address

CSIRT Synacktiv offices are located in France:

- Paris (headquarters) : 5, boulevard montmartre, 75002 Paris
- Rennes : 38 avenue Andrée Viollis, 35000 Rennes
- Toulouse: 11 rue des Abeilles, 31000 Toulouse
- Lyon: 56 rue Smith, 69002 Lyon

2.3. Time Zone

Romance Standard Time (RST)

2.4. Telephone Number

CSIRT number (French prefix) : +33 9 7118 2769

Office number (French prefix) : +33 1 4579 7475

2.5. Facsimile Number

n/a

2.6. Other Telecommunication

A secure portal called SES is available to transfer data in addition to email (large volume) like evidence.

2.7. Electronic Mail Address

Communication from other CSIRT/CERT or if you experienced an incident and need support from Synacktiv

cisrt@synacktiv.com

2.8. Public Keys and Encryption Information

Fingerprint : D9F6 341D 0C48 B469 C57E AD78 0063 A045 942D 2A89

Key ID : 0x0063A045942D2A89 2021-09-15 [expire : 2022-09-15]

User ID : CSIRT Synacktiv <csirt@synacktiv.com>

https://www.synacktiv.com/sites/default/files/2022-10/csirt_synacktiv.txt

2.9. Team Members

- Arnaud Pilon <arnaud.pilon@synacktiv.com> : team leader of the Incident Response Team
- Team members not publicly available

2.10. Other Information

https://www.synacktiv.com/ for other information.

2.11. Points of Customer Contact

CSIRT Synacktiv is the operational point of contact only during business hours. Out of business hours requests are processed only for registered clients. For any commercial purpose, sales@synacktiv.com

3. Charter

3.1. Mission Statement

CSIRT Synacktiv is committed to provide assistance to our new or existing customers. Incident responders provide assistance to understand and investigate incidents and help to mitigate the attack. Renowned for its offensive capabilities, CSIRT Synacktiv give a refreshing understanding of threat actors and their TTP. CSIRT Synacktiv is a consulting company not affiliated or linked with a dedicated commercial vendor.

3.2. Constituency

Any customer with an IT-related incident can ask CSIRT Synacktiv for an incident response service as described on the website www.synacktiv.com. Public or Private sector.

3.3. Sponsorship and/or Affiliation

CSIRT Synacktiv is part of Synacktiv a French company full owned by the two founders Renaud Feil (CEO) and Nicolas Collignon (CTO).

3.4. Authority

Renaud Feil (CEO) and Nicolas Collignon (CTO).

4. Policies

4.1. Types of Incidents and Level of Support

CSIRT Synacktiv handle any kind of IT-related security incident (phishing, apt, malicious user, malware / exploit analysis, etc.) from various perimeter (on-premise, cloud, Windows, Linux, smartphone,…). Synacktiv services are open in business hours and any request is processed in 6 hours.

4.2. Co-operation, Interaction and Disclosure of Information

CSIRT Synacktiv do not share or disclose information of incident response without the consent of its customers. TLP (https://www.first.org/tlp) is used to share data to partners or legal entities.

All of our investigation are processed and stored in France.

4.3. Communication and Authentication

- Encrypted email with GPG can be used for sensitive information / incidents
- Secure transfer service (HTTPS) is available for large volumes

5. Services

5.1. Incident Response

- Incident response : standard service to investigate and remediate incident or verify an incident occurred
- Preparation : help IT teams to increase the log level of critical system and operational awareness
- Implant assessment : software and hardware verification of implant in a dedicated system

5.2. Proactive Activities

- Compromised assessment : proactively hunt undetected incident by standard means
- On-demand training

6. Incident Reporting Forms

If you request CSIRT Synacktiv, we recommend sending an encrypted email to csirt@synacktiv.com and describe relevant information of the security incident :

- What : the scope and type of suspected or compromised systems
- When : a timeline of key known elements
- Who : the name of the people affected by the incident, first IOC, ...
- Where : the physical location of the affected systems or the cloud provider (region)

A phone call is usually followed up to complete and fill out the understanding of the incident.

7. Disclaimers

n/a