CSIRT Talex

RFC-2350

About this document

Title:	Version:	Date of publication:
RFC-2350 CSIRT Talex	1.0	17.03.2020

1. About this document

1.1. Date of Last Update

This is version 1.0, published on 17 March 2020.

1.2. Distribution List for Notifications

Currently no notifications about changes in this document are published using any distribution lists.

1.3. Locations where this Document May Be Found

The current version of this document is available from the Talex S.A. WWW site; its URL is *https://www.talex.pl/en/CSIRT*.

1.4. Authenticating this Document

This document has been signed with the Talex S.A. PGP key. The PGP key can be found on the following Web site: *https://www.talex.pl/en/CSIRT*.

2. Contact Information

2.1. Name of the Team

CSIRT Talex

2.2. Address

CSIRT Talex
Talex S.A.
ul. Karpia 27d
61-619 Poznań
Poland

2.3. Set-up date

CSIRT Talex was established in December 2017.

2.4. Time Zone

Central European Time (CET)
GMT +0100 from November to March
GMT +0200 from April to October

2.5. Telephone Number

+48 61 827 55 00

2.6. Facsimile Number

+48 61 827 55 99

2.7. Other Telecommunication

None available.

2.8. Electronic Mail Address

Please send information about incident to <csirt(at)talex.pl>.

2.9. Public Keys and Other Encryption Information

All sent e-mail communication is encrypted using the PGP (Pretty Good Privacy) mechanism.

The SCIRT Talex public key and its signature are available under the following address: *https://www.talex.pl/en/CSIRT*

2.10. Members of the Team

The CSIRT Talex team is comprised of dedicated cybersecurity experts with many years of experience in this and associated fields of IT.

2.11. Points of Customer Contact

The preferred form of contact is via email to <csirt(at)talex.pl>. We encourage our customers to send us messages encrypted using the PGP key indicated in this document. in situations where immediate contact is necessary, please call the phone number +48 61 827 55 00. We can be reached by telephone during regular office hours in Poland.

3. Charter

3.1. Mission Statement

The CSIRT Talex team considers as its mission to provide cost-friendly cybersecurity services and to prevent and respond to IT security incidents affecting the Company and its clients.

3.2. Constituency

CSIRT Talex provides support to the Company and its clients.

3.3. Sponsorship and/or Affiliation

CSIRT Talex is a commercial entity acting as a part of the Talex S.A. company.

3.4. Authority

CSIRT Talex acts under the authority and auspices of the Management Board of the Talex S.A. company.

4. Policies

4.1. Types of Incidents and Level of Support

CSIRT Talex is authorized to handle all cybersecurity incidents occurring in the IT environments of the Company and its clients (within the scopes set forth in agreements).
Incident notifications transferred to CSIRT Talex will be analysed, classified, and prioritized in accordance with the adopted rules. The level of support shall vary depending on the apparent severity of the incident, its scope, and available resources. In the case of notifications transferred as part of the services provided by CSIRT to the Company's clients, he level of support and incident handling time stem from the provisions set forth in the agreements covering these services.

4.2. Co-operation, Interaction, and Disclosure of Information

CSIRT Talex declares its will to co-operate with other CERT/CSIRT teams and the employees of the Company's clients. All data transmitted to CSIRT Talex is protected pursuant to the Polish and European acts of law. No personal data shall be exchanged without the express permission of the interested party. All information transmitted further is anonymised.

4.3. Communication and Authentication

All transmission of sensitive data should be encrypted, preferably using the PGP mechanism The repository for the PGP keys of CSIRT Talex is indicated in section 2.9. Non-encrypted channels are considered acceptable for low-sensitivity operational communication.

Before establishing a channel of communication, the originator will be authenticated through the PGP key verification or using available identity verification methods (e.g., direct contact).

CSIRT Talex supports communication using the Traffic Light Protocol (TLP) *set of rules.* Electronic messages containing sensitive data should be tagged according to the TLP standard.

5. Services

5.1. Incident Response

CSIRT Talex will provide services for the administrators and clients of the Company in the following areas:

5.1.1. Incident Triage

- analysis to determine the authenticity of a given event,
- classification and prioritization of the incident.

5.1.2. Incident Coordination

- determining the initial cause and extent of the incident,
- collection and categorization of data for analysis,
- notifying parties involved in handling the incident,
- composing announcements to end users,
- making reports.

5.1.3. Incident handling

- removing the cause of the incident,
- support in incident recovery,
- preserving and collecting evidence for possible investigation,
- preparing "Lesson learning" recommendations for administrators.

5.2. Proactive Services

The CSIRT Talex team strives to actively prevent incidents through the following proactive services:

- improving correlation rules in order to improve future detection of incidents of the same type,
- communications and e-learning activities for the employees of the Company and its clients to raise awareness concerning cybersecurity,

- collecting and analysing information, as well as sending notifications about detected threats to the administrators of the Company and its clients,
- consulting in the areas of technology, IT work organization, and cybersecurity,
- vulnerability scanning.

6. Security Incident Reporting

Security incident reports should be sent to the e-mail address mentioned in section 2.11. Reports addressed to CSIRT Talex should at least contain the information about the affected systems, date and time of occurrence, event description, and an indication whether they involve Talex S.A. or its clients.

7. Disclaimers

While CSIRT Talex shall endeavour to prepare correct and adequate information, notifications, and alerts, it does not assume responsibility for possible errors and omissions, or for damages resulting from the use of information contained within.