Description of Telindus-CSIRT

Telindus CyberSecurity Incident Response Team

telindus
powered by tango

together with
proximus

Issued on 02 October 2018

Version: 2.6

Contact: csirt@telindus.lu

Sensitivity: PUBLIC

TLP: White

Table of contents

1 About this document

This document is the description of CyberSecurity Incident Response Team of Telindus S.A. also known as Telindus-CSIRT. This description is performed in line with the rfc2350 document entitled *Expectations for Computer Security Incident Response*. It provides general information about the computer security incident response team (CSIRT) of Telindus S.A., its contact information, its scope of responsibilities, the procedures to contact the team, the set of services offered and how to report an incident.

1.1 Date of last update

This is version 2.6, issued on 2018-10-02

This version is valid until superseded by a later version.

Changes between two successive versions are marked with a vertical line.

Versioning:

1.0	2015-09-22	2.0	2016-02-03
1.1	2015-10-16	2.1	2016-04-11
1.2	2015-10-28	2.2	2017-03-08
1.3	2015-12-01	2.3	2017-06-16
		2.4	2017-09-01
		2.5	2017-10-09
		2.6	2018-10-02

1.2 Distribution list for notifications

Currently Telindus S.A. does not use any distribution list to notify about changes in this document.

In case of questions or remarks about this document, address them to Telindus-CSIRT e-mail address (refer to section 2.6)

1.3 Location where this document may be found

The up-to-date current version of this CSIRT description document is available at the Telindus-CSIRT website at:
https://www.telindus.lu/fr/cybersecurity-incident-response-team or https://www.telindus.lu/en/cybersecurity-incident-response-team

Please make sure you are using the latest version.

Printer and paper versions are not managed.

1.4 Authenticating this document

This document has been signed with the Telindus-CSIRT's PGP key.

The signature is on our web site, under https://www.telindus.lu/fr/cybersecurity-incident-response-team or https://www.telindus.lu/en/cybersecurity-incident-response-team

2 Contact information

2.1 Name of the team

Telindus Cyber Security Incident Response Team

Short name: Telindus-CSIRT

2.2 Address

Telindus-CSIRT

c/o Cybersecurity Services (Cédric MAUNY)

81-83 route d'Arlon

L-8009 Strassen

Grand Duchy of Luxembourg

2.3 Time zone

Central European Time (GMT+0100, GMT+0200 from April to October)

2.4 Telephone number

+352 450 915 - 1

2.5 Facsimile number

+352 450 911

2.6 Electronic mail address

Incident reports, notification and/or any CSIRT related communications should be addressed to `csirt(at)telindus(dot)lu`.

Operational issues should be addressed to `telecomsd(at)telindus(dot)lu`.

2.7 Other telecommunication

Telindus S.A. generic email address is `contact(at)telindus(dot)lu`.

The abuse contact information email address for Autonomous System Number (ASN) `AS56665` is `abuse(at)proximus(dot)lu`.

2.8 Public keys and other encryption information

Telindus-CSIRT has an OpenPGP public key, whose KeyID is `6E2EA9F8` and whose fingerprint is `B6FB 4A00 5437 BA53 69D2 C379 F121 EBA2 6E2E A9F8`.

Each Telindus-CSIRT team member has also a respective OpenPGP public key that you can also fetch from the Telindus-CSIRT's website and from public key servers.

2.9 Team members

Telindus-CSIRT is operated by Telindus S.A. engineers and consultants under the hospice of the Director of Services Delivery. The Core-Team (in alphabetical order) is composed of:

Name	Email	PGP Fingerprint
Joany BOUTET	joany.boutet(at)telindus(dot)lu	A792 3B9B 6A81 C2A0 2CDB FE1B 7821 F5BD 8435 FE90
Sebastien GRELOT	sebastien.grelot(at)tangoservices(dot)lu	9D08 959A AC27 5FCB C2C4 ECCA 79C8 C5D5 8B8F A98C
Frédéric HAUSS *SOC Leader*	frederic.hauss(at)telindus(dot)lu	C20A 604D 86A9 B04E 202A 38C9 9C14 F308 FF59 04CE
Jean-François JOB *Security Operations Leader*	jeanfrancois.job(at)telindus(dot)lu	B5AD 8ABE 4247 BFC8 93A2 CCA4 9366 3C44 0917 F7F1
Cédric MAUNY *Cybersecurity & CSIRT Leader*	cedric.mauny(at)telindus(dot)lu	6F24 CD91 0D60 B8C8 7779 E102 71A9 07DB CAB5 8406
Gilles MULHEIMS	gilles.mulheims(at)tangoservices(dot)lu	_
Jérémy THIMONT	jeremy.thimont(at)telindus(dot)lu	21BA 2119 80A3 2CC4 2C70 A42E 23F3 3E87 F462 401B

2.10 Other information

Any other information about Telindus-CSIRT can be found at https://www.telindus.lu/fr/cybersecurity-incident-response-team or https://www.telindus.lu/en/cybersecurity-incident-response-team

General information about Telindus S.A. can be found at http://www.telindus.lu.

2.11 Points of customer contact

The preferred method for contacting Telindus-CSIRT is via e-mail at `csirt(at)telindus(dot)lu`. We encourage our constituency (customers) to use PGP encryption when sending any sensitive information to Telindus-CSIRT.

If it is not possible (or not advisable for security reasons) to use e-mail, Telindus-CSIRT can be reached by telephone during regular office hours. Off these hours, a voicemail message proposes a redirection to a third party phone number, who will transmit the message to Telindus S.A.

Telindus-CSIRT hours of operation are restricted to regular business hours: 09h00-17h00 CET from Monday to Friday except during Luxembourg's public holidays.

Outside of these hours and in case of emergency, the `telecomsd(at)telindus(dot)lu` email address, mainly dedicated to operational problems, can be contacted.

When submitting your incident report, please use the form mentioned in section 0.

3 Charter

3.1 Mission statement

Telindus-CSIRT is the response entity for the cybersecurity and computer security incidents related to the Autonomous System Number (ASN) AS56665.

Mission of Telindus-CSIRT is to provide the following set of information security incident management related services to its constituency:

- provide a response facility to ICT-incidents,
- setup of a Central-Point-of-Contact for ICT-Incidents between Telindus S.A., its constituency and various CSIRTs,
- support Telindus S.A. internal operational teams to respond from ICT-incidents,
- coordinate communication among various incident response teams,
- provide security expertise and advice.
-

3.2 Constituency

Telindus-CSIRT is responsible for the Autonomous System Number (ASN) AS56665 also known as ASN-Telindus-Telecom and covers services that Telindus S.A. offers to its customers and to its employees (ISP customers base and Commercial organization).

The full AS56665 is owned by Telindus S.A. however, it includes IP addresses that are statically assigned to customers for which Telindus S.A. will not intervene outside of the legal framework that we are bound to operate in.

Consequently, the Telindus S.A.'s customers using IP address(es) belonging to the Autonomous System AS56665 are all included in the constituency of Telindus-CSIRT wherever their physical location.

Our scope of activities covers incidents originated from or targeted the Autonomous System AS56665. All related incidents happening within the AS itself may not be taken into account in the scope of the covered incidents but Telindus-CSIRT can also provide incident response coordination and support to the extent possible depending on its resources.

Telindus-CSIRT may not have the authority to respond to every reported security events, vulnerabilities and incidents related to AS56665 and associated ranges of IP addresses. In particular, Telindus-CSIRT does not have the mandate to intervene for responding[1] to information security incidents and vulnerabilities that are occurring on infrastructures, components and information systems not owned by Telindus S.A. In particular that means that equipment owned by our customers does not fall in the scope of Telindus-CSIRT's responsibilities. However, in such a case and depending on the situation and to the extent possible depending on its resources, Telindus-CSIRT may coordinate and/or support the incident response and vulnerability response and alerts & warning

[1] (Collection, Detection, Assessment, Qualification, Confirmation) Containment, Eradication and Recovery

services with the interested parties in compliance with the Law.

The services proposed in section 0 can also be subscribed by any past, current or future customer of Telindus S.A.

3.3 Sponsorship and/or Affiliation

Telindus-CSIRT is a private CSIRT, defined, owned and operated by Telindus S.A. from the territory of the Grand-Duchy of Luxembourg.

Telindus-CSIRT maintains relationships and affiliations with the public and private CSIRT members of the CERT.lu initiative in Luxembourg.

Telindus-CSIRT has been established on 2015, September 22nd, *Listed* by Trusted-Introducer since 2015, October 15th and is currently *Accredited* since 2016, March 25th.

3.4 Authority

Telindus-CSIRT operates under the auspices of, and with authority delegated by Telindus S.A.

4 Policies

4.1 Types of incidents and level of support

Telindus-CSIRT is authorized to address all types of computer and information security incidents which occur or threaten to occur, within its constituency.

The level of support given by Telindus-CSIRT varies depending on the type and severity of the incident or issue, the type of the impacted constituent, the size of the user community affected, and Telindus-CSIRT's resources at the time; though in all cases some response will be made.

Incidents will be prioritized according to their apparent severity and extent.

End-users are expected to contact their security point of contact, systems administrator, network administrator or department head for assistance. Telindus-CSIRT aims in providing support in the frame of its services and abilities to the system administrators, network administrators or department heads within the limit of its constituency and services. No support is provided to the end-user by Telindus-CSIRT.

4.2 Co-operation, interaction and disclosure of information

As operated by Telindus S.A., Telindus-CSIRT shall comply with same regulations applicable to Telindus S.A. Therefore, Telindus-CSIRT exchanges necessary information with other CSIRTs as well as with Constituents' and affected parties' security point-of-contact in accordance with regulations applicable to Telindus S.A. Those applicable regulations include but not limited to

- Luxembourgish sector-specific Regulations and Rules of CSSF (Commission de Surveillance du Secteur Financier) considering Telindus S.A. is acting as support FSP (Financial Sector Professional)
- ILR (Institut Luxembourgeois de Régulation) considering Telindus S.A. is acting as telecom operator in Luxembourg.

When co-operating, interacting and disclosing information, other Luxembourg's local rules and legislation are also taken into consideration by Telindus-CSIRT and concern:

- Data protection and privacy of personal information
  - Law of 2 August 2002 for protection of personal data.
- Electronic communications services and networks
  - Laws of 27 February 2011 (the Paquet Telecom) designed to provide set of rules for the entire electronic communication services and networks.
- Any other specific laws and regulations applying to our customer's activities.

Telindus-CSIRT recognises and supports Information Sharing Traffic Light Protocol[2] and appends it when sharing information with

[2] As specified at https://www.first.org/tlp/docs/tlp-v1.pdf

teams that support it, and will honour such information if present. All sensitive data (such as but not limited to personal data, system configurations, and known vulnerabilities with their locations) are encrypted if they have to be transmitted over unsecured environment, as stated below.

4.3 Communication and authentication

In view of the types of information that Telindus-CSIRT deals with, telephones 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 low-sensitivity data.

If it is necessary to send highly sensitive data by e-mail, encryption (preferably PGP) will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

All e-mail or data communication originating from Telindus-CSIRT will be digitally signed, using the generic PGP key mentioned above or the Telindus-CSIRT agents' own signature keys.

If deemed necessary, especially when there is need to exchange high volume of information, Telindus-CSIRT could also use repository systems as alternative communication means. Such repositories will always be provided in line with the above mentioned secure approach. Such repository systems will be owned, managed and hosted by Telindus S.A. in line with applicable Regulations applicable to Telindus S.A.

5 Services

The set of services listed and described below are either performed by member of the core-team of Telindus-CSIRT or subcontracted to specialised teams at Telindus S.A. to the extent possible depending on its resources.

5.1 Reactive services

In line with the generic description of CSIRT Services[3] maintained by the CERT Division of the *Software Engineering Institute (SEI)* of Carnegie Mellon University, Telindus-CSIRT proposes and provides the set of following reactive services:

- Alerts and Warnings
- Incident handling
  - Incident analysis
  - Incident response support
  - Incident response coordination
- Vulnerability handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination

5.2 Proactive services

In line with the generic description of CSIRT Services[3] maintained by the CERT Division of the *Software Engineering Institute (SEI)* of Carnegie Mellon University, Telindus-CSIRT proposes and provides the set of following proactive services to the extent possible depending on its resources:

- Announcements
- Technology watch
- Security audits or assessments
  - Infrastructure review
  - Best practice review
  - Scanning
  - Penetration testing
  - Security and network equipment configurations audit
  - Source code review
- Configuration and maintenance of security tools, applications, and infrastructures

[3] https://www.cert.org/incident-management/services.cfm

5.3 Security quality management services

In line with the generic description of CSIRT Services[3] maintained by the CERT Division of the *Software Engineering Institute (SEI)* of Carnegie Mellon University, Telindus-CSIRT proposes and provides the set of following security quality management services to the extent possible depending on its resources:

- Risk Analysis
  - Identify and assess your risks an evaluate security posture of your assets
  - Prioritize your security investments, providing optimal security in a cost effective manner by efficient resources management
- Security consulting
  - For governance
    - Align your information security program activities with organizational goals and business priorities
    - Ensure security management and activities contributes to the process of value creation
  - For compliance
    - Translate regulatory requirements into effective and practicable security policies and controls
    - Lever compliance investments to increase the effectiveness of security controls
- Awareness building
  - Protect your assets by raising information security awareness of your staff
- Education/Training
  - Increase business value by improving the knowledge and skills of your staff
- Security infrastructure management
  - Assistance for security architecture design.
  - Implementation of security infrastructures and security devices
  - Expertise, engineering, installation, configuration and maintenance of security solutions
  - Maintenance of security solutions
  - Security audits and review of security solutions
  - Logs analysis
- Ethical hacking
  - Vulnerability assessment and evaluation
  - Penetration testing
  - Source code review
  - Social engineering

According to the specificities of these services, some may be outsourced to internal security consultancy departments of Telindus S.A. or any other departments of Telindus S.A. such as the Telindus Training Institute relevant for the different services provided.

6 Incident reporting form

Telindus-CSIRT has created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out.

> The current version of the form is available at https://www.telindus.lu/fr/cybersecurity-incident-response-team or https://www.telindus.lu/en/cybersecurity-incident-response-team

7 Disclaimer

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