Proximus Ada Cyber Security Incident Response Team

RFC 2350 Description

Date	02/05/2022
Sensitivity	Unrestricted
Our reference	PXS-CSIRT-RFC2350-v1.7
Contact	Krystina Vrublevska
E-mail	krystina.vrublevska@proximus-ada.com

Table of contents

1. Document Information

This document provides formal description of the PXS Ada CSIRT based on RFC 2350.

1.1 Date of Last Update

This is version 1.7, published on the 03/12/2021.

1.2 Distribution List for Notifications

Notifications can be sent to csirt@proximus-ada.com

1.3 Locations where this Document may be found

http://www.proximus.com/csirt

1.4 Authenticating this Document

Document should carry a valid PGP signature of the CSIRT Manager in order to assure its authenticity.

2. Contact Information

2.1 Name of the Team

PXS Ada CSIRT – Proximus Ada Cyber Security Incident Response Team

2.2 Address

K. Albert-II Laan 27 B-1030 Brussels, Belgium

2.3 Time Zone

GMT+1 (CET)

2.4 Telephone Number

+32 (0)7 805 01 61

2.5 Facsimile Number

Not available.

2.6 Other telecommunications

Not available.

2.7 Electronic Mail Address

csirt@proximus-ada.com

2.8 Public Keys and Encryption Information

E-mail address: csirt@proximus-ada.com

Key ID: 5D0B022A7CFBC5B3

Length: 2.048

Fingerprint: 8671 CBF3 C010 E4F0 676A 9CD7 5D0B 022A 7CFB C5B3

2.9 Team members

Krystina Vrublevska

krystina.vrublevska@proximus-ada.com (for general usage)

krystina@proximus.security (for PGP encrypted mail)

Lieven de Smaele

lieven.de.smaele@proximus-ada.com (for general usage)

lieven@proximus.security (for PGP encrypted mail)

Key ID: 0x1162DC4AFC4C2584

Fingerprint: 3575 1F63 6AB1 B55A CE19 49C1 1162 DC4A FC4C 2584

Jeremy Schmidt

jeremy.schmidt@proximus-ada.com (for general usage)

jeremy@proximus.security (for PGP encrypted mail)

Key ID: 0x724D1092374AACE2

Fingerprint: 0BDD 3E42 877F CC8C 95B4 93CC 724D 1092 374A ACE2

Mathieu Allaert

mathieu.allaert@proximus-ada.com (for general usage)

mathieu@proximus.security (for PGP encrypted mail)

Key ID: 0x71AE24BF3045DECC

Fingerprint: DEE9 A048 0A88 C1AA 596D AD5C 71AE 24BF 3045 DECC

Hanne Peeters

hanne.peeters@proximus-ada.com (for general usage)

hanne@proximus.security (for PGP encrypted mail)

Key ID: 0x8B7C183D8307152D

Fingerprint: B6DF ABC8 66E9 6798 7327 C338 8B7C 183D 8307 152D

Rajendra Mekhale

rajendra.mekhale@proximus-ada.com (for general usage)

rajendra@proximus.security (for PGP encrypted mail)

Key ID: 0x69B67C6CAFC35CCD

Fingerprint: 0B83 E0F5 7452 3AE7 C92A 808E 69B6 7C6C AFC3 5CCD

2.10 Points of Customer Contact

The preferred method for contacting PXS-ADA-CSIRT is via e-mail csirt@proximus-ada.com. If it is not possible (or not advisable for security reasons) the PXS-ADA-CSIRT can be reached by phone (see Telephone Number) during extended business hours from 07.00 until 18.00.

3. Charter

3.1 Mission Statement

The Proximus CSIRT (PXS-CSIRT) is the central incident response team of the Proximus Group and its mission is to provide information and assistance to reduce the risks of cyber security incidents as well as responding effectively to such incidents when they occur. The team strives to be an international example for Cyber Security Intelligence and Expertise throughout all areas of Incident Response. The Proximus CSIRT gathers, filters, analyses and disseminates threat intelligence in order to proactively communicate about upcoming attacks against the Proximus Group.

3.2 Constituency

The constituency of the PXS-CSIRT is two-fold:

- ISP-customers & commercial-customers: services that Proximus offers.
- Commercial organization: employees of the Proximus Group

The PXS-CSIRT is not intervening for cyber security incidents, that are not occurring on Proximus managed infrastructure. That means that consumer equipment (e.g., laptop) does not fall in the scope of the PXS-CSIRT's responsibilities. Affiliates (Telindus NL, Telindus UK, Telindus LU, Tango LU, BICS) are part of the commercial-organization constituency.

In general, the full AS5432 is owned by Proximus. However, these also include IP addresses that are statically or dynamically assigned to customers for which Proximus will not be intervene outside of the legal framework that we are bound to operate in.

3.3 Sponsorship and/or Affiliation

The Proximus Group Information Security Steering Committee (GISSC) led by the Proximus CISO and consisting of Directors of all internal divisions has mandated a full authority to the PXS-CSIRT to immediately mitigate the impact of any cyber security incident.

3.4 Authority

As per the mandate of the GISSC, in order to immediately mitigate the impact of a cyber security incident, the Proximus CSIRT has full authority to implement corrective controls, within the legal and regulatory framework it is bound to work in. PXS-CSIRT is reporting directly to Proximus CISO, who reports to Proximus executive committee – and remains to have full authority and mandate for mitigating any kind of cyber security incident within their constituency.

4. Policies

4.1 Types of Incidents and Level of Support

The PXS-CSIRT is classifying all incidents, based on the following categories:

Unauthorized Access	**Denial of service**	**Vulnerability exploitation**
Data Disclosure	**Malicious code**	**Brand protection**
Spam	**Social engineering**	**Policy violation**

Any incident reports that do not fall under any of these 9 categories, will be handled and prioritized, based on their impact.

Target service level for responding to any incidents reported to the PXS-CSIRT is 90% within 1 business day.

4.2 Co-operation, Interaction and Disclosure of Information

The Proximus CSIRT is actively participating within the ETIS EU CERT group, which consists of Telco CERT group throughout Europe. This information-sharing working group is mainly focusing on incidents that have been reported and analysed by the different CERT teams. In addition to ETIS, the Proximus CSIRT is also an active member of the FIRST and Trusted Introducer communities.

Nationally, Proximus is one of the founding members of the Cyber Security Coalition where the Proximus CSIRT leads the Inter-CSIRT working group. There is also active collaboration with the national CERT in Belgium (CERT.BE), as well as different Law Enforcement Agencies, (military) intelligence services, regulatory bodies, etc.

Next to the corporate security policy on data classification (used internally) the PXS-CSIRT applies the Traffic Light Protocol for information that is shared and/or distributed with trusted parties.

All incident-related communication with other CERTs will be tagged with a unique identifier, referring to the incident number, as recorded in the PXS-CSIRT incident management system.

Communication with constituencies will be primarily via e-mail, in close collaboration with Internal Communication and/or Proximus Press team.

4.2.1 RED - personal for named recipients only

In the context of a meeting, for example, red information is limited to those present at the meeting. In most circumstances, red information will be passed verbally or in person.

4.2.2 AMBER - limited distribution

The recipient may share AMBER information with others within their organization, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.

Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community.

4.2.3 GREEN – peers and partners, non-public

GREEN may be shared with peers and partner organizations within their sector or community, but not via publicly accessible channels.

4.2.4 WHITE - unlimited

WHITE may be distributed without restriction, subject to copyright controls.

4.3 Communication and Authentication

All communication that is above "green" must be transmitted through secure channel only.

5. Services

5.1 Reactive Services

- Alerts & warnings
- Incident handling
- Incident analysis
- Incident response
- Incident response support
- Incident response on-site
- Incident response coordination
- Responsible disclosure
- Artefact coordination
- Artefact analysis
- Artefact response
- Forensic analysis
- Vulnerability management

5.2 Proactive Services

- Announcements
- Development of security tools
- Intrusion detection services
- Technology watch
- Trend and neighbourhood watch
- Security-related information dissemination

5.3 Quality Management Services

- Awareness building
- Education & training
- Threat analysis
- Security consulting

6. Incident Reporting Forms

E-mail only