proximus NXT
cybersecurity

Proximus Luxembourg CyberSecurity Incident Response Team

Incident Notification Form

Created on 21/07/26 | Version 4.0 | Sensitivity: Public | TLP: CLEAR

The Proximus Luxembourg CSIRT (**PXS-LU-CSIRT**) is the response entity for the computer incidents related to the Autonomous System Number (ASN) **AS56665**.

To report a security incident, please complete this form as thoroughly as possible and send it to csirt (at) proximus (dot) lu - preferably PGP/GPG encrypted (PGP KeyID 6E2EA9F8).

PXS-LU-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 email telecomsd (at) proximus (dot) lu address, mainly dedicated to operational problems, can be contacted.

All reported information will be treated confidentially according to our policies (please refer to our rfc2350 available at https://www.proximusnxt.lu/en/csirt).

IMPORTANT REMINDERS

- File a complaint with legal authorities (Police Grand-ducale, Parquet du Luxembourg) if applicable.
- If personal data was compromised, notify the CNPD within 72 hours (GDPR).
- If the affected entity falls under DORA, assess whether this qualifies as a major ICT-related incident requiring regulatory notification.
- All information is treated confidentially per our RFC 2350 policy.

SECTION 1 - About the Reporter

Organization / Company

Contact Name / Job Title

Contact Name	Job Title / Role

Phone Number / Email Address

Phone Number	Email Address

SECTION 2 - Incident Classification

Date / Time Detected & Date Reported

Date Detected	Time Detected	Date Reported

Type of Incident

Select all that apply.

☐ Unauthorized Access	☐ Denial of Service
☐ Vulnerability Exploitation	☐ Data Breach / Disclosure
☐ Malicious Code / Malware	☐ Ransomware
☐ Phishing / Spam	☐ Social Engineering
☐ Brand / Identity Abuse	☐ Policy Violation
☐ Insider Threat	☐ Supply Chain Compromise
☐ Other (specify below)	

If "Other", please specify:

Severity Level

☐ Critical	☐ High
☐ Medium	☐ Low
☐ Unknown	

Current Status

☐ Occurring	☐ Contained
☐ Occurred	☐ Unknown

SECTION 3 - Affected Systems & Infrastructure

Impacted System(s) / Hostname(s)

IP Address(es) / Range(s) & Operating System(s)

IP Address(es) / Range(s)	Operating System(s)

Affected Services / Applications

Network Segment / VLAN (if known)

SECTION 4 - Indicators of Compromise (IoC)

Suspicious IP Addresses / Domains / URLs

File Hashes (MD5 / SHA-1 / SHA-256)

Malware Samples / Names (if identified)

Suspicious Email Addresses / Subjects

SECTION 5 – Impact Assessment

Data Affected

☐ Personal Data (GDPR)	☐ Financial Data
☐ Intellectual Property	☐ Credentials / Secrets
☐ None / Unknown	

Estimated No. of Affected Users / Records & Business Impact

Estimated No. of Affected Users / Records	Business Impact

Has the CNPD been notified?

☐ Yes	☐ No
☐ Not applicable	

Does this incident require DORA major-incident notification?

Applicable if the affected entity or service is in scope of Regulation (EU) 2022/2554.

☐ Yes	☐ No
☐ Not applicable / Unknown	

SECTION 6 - Incident Description

Detailed Chronological Account

Describe what happened, when, how it was detected, and what is currently known.

SECTION 7 - Actions Already Taken

Containment, Eradication & Mitigation Steps

Describe containment, eradication, or mitigation steps already performed.

SECTION 8 - Supporting Evidence & Attachments

Attached Materials

Select all that apply.

☐ Log files	☐ Screenshots
☐ Network captures (PCAP)	☐ Malware samples
☐ Email headers	☐ Other

CONFIDENTIALITY NOTICE

All reported information will be treated confidentially in accordance with PXS-LU-CSIRT policies (RFC 2350). See https://www.proximusnxt.lu/en/csirt

SUBMISSION INSTRUCTIONS

Please send this completed form along with any attached evidence to csirt (at) proximus (dot) lu. PGP/GPG encryption is strongly recommended (PGP KeyID: 6E2EA9F8).