Telindus-CSIRT

Telindus CyberSecurity Incident Response Team

Incident Reporting Form

Immediately fill a complaint if you are the victim of a cyberattack, get closer to legal authorities in Luxembourg.

- Police Grand-ducale du Luxembourg
- Parquet du Luxembourg (Parquet du Tribunal d'Arrondissement du Luxembourg et Parquet du Tribunal d'Arrondissement de Diekirch)
- Service de la Police Judiciaire, Section Nouvelles Technologies, Luxembourg

In case of positive identification of a compromised server, don't forget to follow the data privacy regulation laws in Europe. It is necessary to identify the problem in detail, identify the leaked personal data and affected people, and contact CNPD[1] within 72 hours to comply with the law and in order to notify the affected people about the leak.

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

To report an incident, please complete as detailed as possible this form and send it to csirt(at)telindus(dot)lu preferably PGP/GPG encrypted (PGP KeyID 6E2EA9F8).

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 email <telecomsd (at) telindus (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.telindus.lu/en/csirt).

[1] *https://cnpd.public.lu/en/professionnels/obligations/violation-de-donnees.html*

Proximus Luxembourg S.A. | 18, rue du Puits Romain – Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 – 1 | F +352 45 09 11 www.proximus.lu

VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO 9001

Incident Reporting Form
Telindus Cyber Security Incident Response Team ~ Telindus-CSIRT

About the reporter	
Company	
Name	
Phone number	
Email address	
About the incident to be reported	
Impacted System(s) / IP Address(es)	
Type of Incident	☐ Unauthorized Access ☐ Denial of service ☐ Vulnerability exploitation ☐ Data Disclosure ☐ Malicious code ☐ Brand protection ☐ Phishing / Spam ☐ Social engineering ☐ Policy violation ☐ Other (precise): ……
Incident Current Status	☐ Occurring ☐ Contained ☐ Occurred ☐ Unknown

Proximus Luxembourg S.A. | 18, rue du Puits Romain – Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 – 1 | F +352 45 09 11 www.proximus.lu
VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO 9001

Reporter's description of the incident Try to be as precise as possible about the description of the incident, its operational impact and all other damages, a first assessment and the actions already taken

Proximus Luxembourg S.A. | 18, rue du Puits Romain – Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 – 1 | F +352 45 09 11 www.proximus.lu

VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO 9001