proximus NXT
cybersecurity

Proximus Luxembourg Cybersecurity Incident Response Team

Vulnerability Notification Form

Created on 12/11/2024 | Version 3.1
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 notify a vulnerability in either software or hardware products, please complete as detailed as possible this form with enough information for allowing PXS-LU-CSIRT and the Vendor to analyse it, understand it and reproduce it 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/proximus-luxembourg-csirt).

Bug Bounty Policy

We value those who take the time and effort to report security vulnerabilities. However, we do not offer monetary rewards for vulnerability disclosures.

Vulnerability Notification Form
Proximus Luxembourg Cyber Security Incident Response Team
~ PXS-LU-CSIRT

About the reporter	
Company	
Name	
Phone number	
Email address	
Remain anonymous	[ ] Yes [ ] No (Default)

About the vulnerability to be notified - Many vulnerabilities can be listed here				
	Vendor	Product	Version Tested	Is vulnerable (yes / no)
Impacted product(s) List the concerned vendors, software / hardware products, version tested and test platform				

Reporter's description of vulnerability

Try to be as precise as possible about the description of the vulnerability, its discovery (tools/techniques), the way to exploit it and the identified potential impacts.