Telindus-CSIRT

Telindus CyberSecurity Incident Response Team
Vulnerability Notification Form

Telindus-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 Telindus-CSIRT and the Vendor to analyse it, understand it and reproduce it and send it to <csirt (at) telindus 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).

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

Telindus Cyber Security Incident Response Team ~ Telindus-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	
Impacted product(s) List the concerned vendors, software / hardware products, version tested and test plateform	

Vendor	Product	Version Tested	Is vulnerable (Yes / No)

Reporter's description of the vulnerability

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