CVE-2002-2133

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2002-2133
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Telindus 1100 ASDL router running firmware 6.0.x uses weak encryption for UDP session traffic, which allows remote attac

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Telindus	1120 Adsl Router	6.0.21b_firmware	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Telindus ADSL Router Encryption Scheme Weakness	af854a3a
archives.neohapsis.com/archives/bugtraq/2003-02/0277.html	af854a3a
archives.neohapsis.com/archives/bugtraq/2002-12/0262.html	af854a3a
ISS X-Force Database: telindus-adsl-weak-encryption (10951): Telindus 1100 series ADSL routers use weak encryption algorithm	af854a3a
www.osvdb.org/4762	af854a3a
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.