CVE-2002-0949

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

Summary

CVE	CVE-2002-0949
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-10-04 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Telindus 1100 series ADSL router allows remote attackers to gain privileges to the device via a certain packet to UDP port 9

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Telindus	Adsl Router	1110	All	All	All

Hardware	Telindus	Adsl Router	1120	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 1100 Series Router Administration Password Leak Vulnerability	af854a3a-
Neohapsis Archives - Bugtraq - Some vulnerabilities in the Telindus 11xx router series - From finelliieee.org	af854a3a-
ISS X-Force Database: telindus-adsl-information-leak (9277): Telindus 1100 series ADSL routers could leak sensitive information	af854a3a-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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