CVE-2002-0672

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

Summary

CVE	CVE-2002-0672
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-07-23 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Pingtel xpressa SIP-based voice-over-IP phone 1.2.5 through 1.2.7.4 allows attackers with physical access to restore the pl

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/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	Pingtel	Xpressa	1.2.5	All	All	All

Hardware	Pingtel	Xpressa	1.2.7.4	All	All	All

Vendor Declared Affected Products

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

References

Reference
www.atstake.com/research/advisories/2002/a071202-1.txt
ISS X-Force Database: pingtel-xpressa-factory-defaults (9567): Pingtel xpressa could allow an attacker to reset the phone to the factory defau
www.pingtel.com/PingtelAtStakeAdvisoryResponse.jsp
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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