



CVE-2002-0675

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

Summary

CVE	CVE-2002-0675
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 does not require administrative privileges to perform a

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				Source		
www.atstake.com/research/advisories/2002/a071202-1.txt				af854a3a-2127-4		
ISS X-Force Database: pingtel-xpressa-firmware-upgrade (9570): Pingtel xpressa allows unauthorized firmware upgrades				af854a3a-2127-4		
Pingtel Expressa Arbitrary Firmware Upgrade Vulnerability				af854a3a-2127-4		
www.pingtel.com/PingtelAtStakeAdvisoryResponse.jsp				af854a3a-2127-4		
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.						