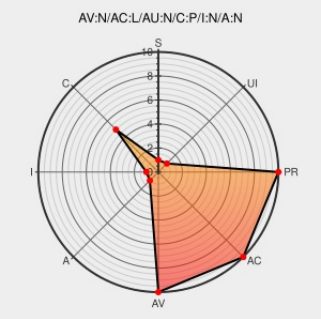
CVE-2002-1934

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1934

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xpressa from Pingtel contain the following vulnerability:

Pingtel xpressa SIP-based voice-over-IP phone 1.2.5 through 2.0.1 leaks sensitive information during boot-up, which allows attackers to obtain the MD5 hash of the Admin password, MD5 hash of the physical password, and other registration information.

CVE-2002-1934 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Pingtel Xpressa Phone Home Information Leakage Vulnerability	cve.report (archive) text/html	BID 5534
ISS X-Force Database: pingtel-xpressa-information-leak (9948): Pingtel xpressa leaks sensitive information upon startup	web.archive.org text/html Inactive Link Not Archived	XF pingtel-xpressa-information-leak(9948)
sys-security.com - This website is for sale! - System security Resources and Information.	Vendor Advisory www.sys-security.com text/plain	MISC www.sys-security.com/archive/advisories/More_Vulnerabilities_with_Pingtel_xpressa_SIP-based_IP_phones.txt
SecurityFocus HOME Mailing List: BugTrag	web.archive.org text/html	BUGTRAQ 20020820 More Vulnerabilities with Pingtel xpressa SIP-based IP phones

Inactive Link Not Archived

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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
Hardware	Pingtel	Xpressa	1.2.8	All	All	All
Hardware	Pingtel	Xpressa	2.0	All	All	All
Hardware	Pingtel	Xpressa	2.0.1	All	All	All
Hardware	Pingtel	Xpressa	1.2.5	All	All	All
Hardware	Pingtel	Xpressa	1.2.7.4	All	All	All
Hardware	Pingtel	Xpressa	1.2.8	All	All	All
Hardware	Pingtel	Xpressa	2.0	All	All	All
Hardware	Pingtel	Xpressa	2.0.1	All	All	All

cpe:2.3:h:pingtel:xpressa:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.7.4:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.7.4:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report