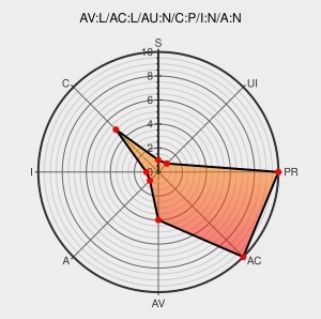
CVE-2005-2664

Published on: 08/22/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2664

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



Certain versions of Whisper32 from Whisper32 contain the following vulnerability:

Whisper 32 1.16, and possibly earlier versions, stores passwords in plaintext in memory, which allows local users to obtain the password using a debugger or another mechanism to read process memory.

CVE-2005-2664 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
	Vendor Advisory, antilamo.skifstone.com, text/plain, Inactive Link, Not Archived	MISC antilamo.skifstone.com/vuln/whisper32.txt
Whisper32 Plaintext Password Disclosure Vulnerability	cve.report (archive), text/html	BID 14600
SecurityTracker.com Archives - Whisper 32 Discloses Password to Local Users	securitytracker.com, text/html	SECTRACK 1014730
'Password Disclosure in Whisper32' - MARC	marc.info, text/html	BUGTRAQ 20050818 Password Disclosure in Whisper32

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
Application	Whisper32	Whisper32	1.16	All	All	All
Application	Whisper32	Whisper32	1.16	All	All	All

cpe:2.3:a:whisper32:whisper32:1.16:*:*:*:*:*:*:*:

cpe:2.3:a:whisper32:whisper32:1.16:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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