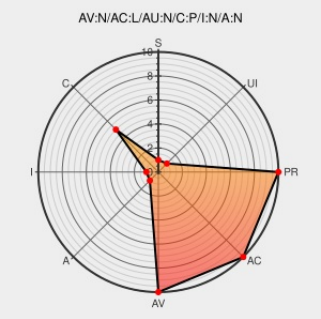
CVE-2006-2021

Published on: 04/25/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:09 PM UTC

CVE-2006-2021

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



Certain versions of Asteriskathome from Asteriskathome contain the following vulnerability:

Absolute path traversal vulnerability in recordings/misc/audio.php in the Asterisk Recording Interface (ARI) web interface in Asterisk@Home before 2.8 allows remote attackers to read arbitrary MP3, WAV, and GSM files via a full pathname in the recording parameter. NOTE: this issue can also be used to determine existence of files.

CVE-2006-2021 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
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060421 [SecuriWeb 2006.1] directory traversal in Asterisk@Home and ARI
SecuriWeb: Ressources/AvisDeSecurite/2006.1	Exploit www.securiweb.net text/html	MISC www.securiweb.net/wiki/Ressources/AvisDeSecurite/2006.1
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF asterisk-audio-directory-traversal(25996)
Secunia - Advisories - ARI Information Disclosure Security Issue and Vulnerability	Exploit Patch Vendor Advisory web.archive.org text/html	SECUNIA 19744

No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24806
Asterisk Recording Interface Audio.PHP Information Disclosure Vulnerability	Exploit Patch cve.report (archive) text/html	BID 17641
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1457
SecurityReason - directory traversal in Asterisk@Home and ARI	securityreason.com text/html	SREASON 750

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
Application	Asteriskathome	Asteriskathome	All	All	All	All

cpe:2.3:a:asteriskathome:asteriskathome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→