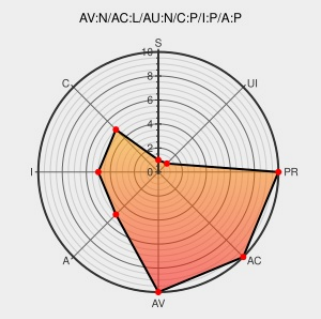
CVE-2005-1240

Published on: 04/20/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

CVE-2005-1240

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



Certain versions of Secure Net from Castlehill contain the following vulnerability:

Directory traversal vulnerability in the third party tool from Castlehill, as used to secure the iSeries AS/400 FTP server, allows remote attackers to access arbitrary files, including those from qsys.lib, via ".." sequences in a GET request.

CVE-2005-1240 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF multiple-vendor-security-bypass(20260)
SecurityFocus	Exploit www.securityfocus.com text/html	BUGTRAQ 20050420 Canonicalization and directory traversal in iSeries FTP security products
	Exploit www.venera.com application/pdf	MISC www.venera.com/downloads/Canonicalization_problems_in_iSeries_FTP_security.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Castlehill	Secure Net	All	All	All	All
Application	Castlehill	Secure Net	All	All	All	All

cpe:2.3:a:castlehill:secure_net:*:*:*:*:*:*:*:*:

cpe:2.3:a:castlehill:secure_net:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→