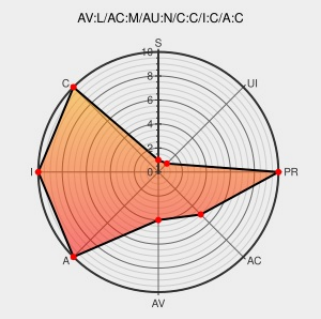
CVE-2010-5250

Published on: 09/07/2012 12:00:00 AM UTC

Last Modified on: 09/06/2022 05:52:00 PM UTC

CVE-2010-5250

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



Certain versions of Pthreads-win32 from Pthread-win32 Project contain the following vulnerability:

Untrusted search path vulnerability in the pthread_win32_process_attach_np function in pthreadGC2.dll in Pthreads-win32 2.8.0 allows local users to gain privileges via a Trojan horse quserex.dll file in the current working directory. NOTE: some of these details are obtained from third party information.

CVE-2010-5250 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Pthreads-win32 Insecure Library Loading Vulnerability - Advisories - Community	Vendor Advisory, web.archive.org, text/html	SECUNIA 41215
DLL Hijacking (KB 2269637) – the unofficial list | Peter Van Eeckhoutte's Blog	web.archive.org, text/html, Inactive Link, Not Archived	MISC www.corelan.be:8800/index.php/2010/08/25/dll-hijacking-kb-2269637-the-unofficial-list/

Related QID Numbers

590725 3S-Smart Software Solutions GmbH CODESYS Control V3 Products Vulnerability (Advisory2016-03_CDS-52287)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pthread-win32 Project	Pthreads-win32	2.8.0	All	All	All
Application	Ross Johnson	Pthreads-win32	2.8.0	All	All	All
Application	Ross Johnson	Pthreads-win32	2.8.0	All	All	All

cpe:2.3:a:pthread-win32_project:pthreads-win32:2.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:ross_johnson:pthreads-win32:2.8.0:*:*:*:*:*:*:*:

cpe:2.3:a:ross_johnson:pthreads-win32:2.8.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→