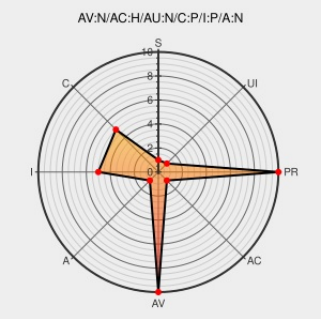
CVE-2006-2297

Published on: 05/09/2006 12:00:00 AM UTC

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

CVE-2006-2297

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



Certain versions of Infotech Storage System Library from Microsoft contain the following vulnerability:

Heap-based buffer overflow in Microsoft Infotech Storage System Library (itss.dll) allows user-assisted attackers to execute arbitrary code via a crafted CHM / ITS file that triggers the overflow while decompiling.

CVE-2006-2297 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory, www.vupen.com, text/html	VUPEN ADV-2006-1761
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20060510 Re: [Reversemode] Microsoft Infotech Storage library Heap Corruption
401 Unauthorized	www.reversemode.com, application/pdf, Inactive Link, Not Archived	MISC www.reversemode.com/advisories/advisory-itss.pdf
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20060512 Re: [Reversemode] Microsoft Infotech Storage library Heap Corruption
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ms-itssdll-chm-bo(26340)

Microsoft Infotech Storage Library Heap Corruption Vulnerability	Exploit cve.report (archive) text/html	BID 17926
Microsoft Infotech Storage library Heap Corruption - CXSecurity.com	securityreason.com text/html	SREASON 886
Microsoft Windows "itss.dll" Heap Corruption Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20061
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060509 [Reversemode] Microsoft Infotech Storage library Heap Corruption
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 25501

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	Microsoft	Infotech Storage System Library	All	All	All	All
Application	Microsoft	Infotech Storage System Library	All	All	All	All

cpe:2.3:a:microsoft:infotech_storage_system_library:*:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:infotech_storage_system_library:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→