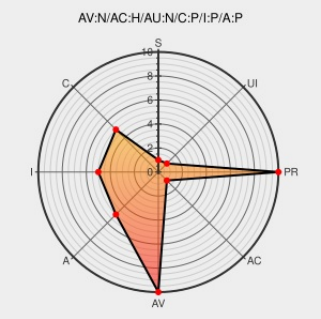
CVE-2004-0475

Published on: 05/20/2004 12:00:00 AM UTC

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

CVE-2004-0475

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



Certain versions of Ie from Microsoft contain the following vulnerability:

The showHelp function in Internet Explorer 6 on Windows XP Pro allows remote attackers to execute arbitrary local .CHM files via a double backward slash ("\\") before the target CHM file, as demonstrated using an "ms-its" URL to ntshared.chm. NOTE: this bug may overlap CVE-2003-1041.

CVE-2004-0475 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityFocus	Exploit, Vendor Advisory, www.securityfocus.com, text/html	BUGTRAQ 20040513 Showhelp() local CHM file execution
Microsoft Internet Explorer Double Backslash CHM File Execution Weakness	Exploit, Vendor Advisory, cve.report (archive), text/html	BID 10348
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ie-showhelp-chm-execution(16147)

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

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	Ie	6.0	sp1	All	All
Application	Microsoft	Ie	6.0	sp1	All	All

cpe:2.3:a:microsoft:ie:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0:sp1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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