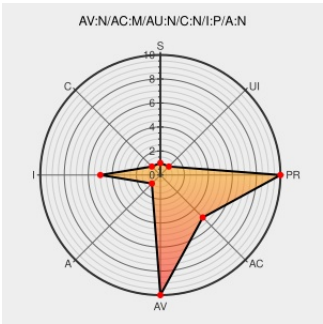
CVE-2007-3576

Published on: 07/05/2007 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:00:00 AM UTC

CVE-2007-3576

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



Certain versions of Ie from Microsoft contain the following vulnerability:

** DISPUTED ** Microsoft Internet Explorer 6 executes web script from URIs of arbitrary scheme names ending with the "script" character sequence, using the (1) vbscript: handler for scheme names with 7 through 9 characters, and the (2) javascript: handler for scheme names with 10 or more characters, which might allow remote attackers to bypass certain XSS protection schemes. NOTE: other researchers dispute the significance of this issue, stating "this only works when typed in the address bar."

CVE-2007-3576 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
sla.ckers.org web application security forum :: XSS Info :: InternetExplorer "javascript/vbscript" aliases	Exploit, web.archive.org, text/xml, Inactive Link, Not Archived	MISC sla.ckers.org/forum/read.php?2,13209,13218
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 45813
No Description Provided	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC ha.ckers.org/blog/20070702/ie60-protocol-guessing/

H Tech Blog | Hack and Evolve Faster with the Common Techniques	Exploit www.0x000000.com text/html	MISC www.0x000000.com/?i=375
Google Groups	Exploit groups.google.com text/html	MISC groups.google.com/group/php-ids/browse_thread/thread/3ec15f69d6b3dba0

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	Ie	6	All	All	All
Application	Microsoft	Ie	6	All	All	All
Application	Microsoft	Internet Explorer	6	All	All	All

cpe:2.3:a:microsoft:ie:6:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→