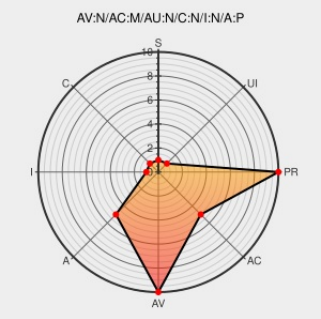
CVE-2003-1505

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 07/23/2021 12:16:00 PM UTC

CVE-2003-1505

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



Certain versions of Ie from Microsoft contain the following vulnerability:

Microsoft Internet Explorer 6.0 allows remote attackers to cause a denial of service (crash) by creating a web page or HTML e-mail with a textarea in a div element whose scrollbar-base-color is modified by a CSS style, which is then moved.

CVE-2003-1505 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	NONE	PARTIAL

CVE References

Description	Tags	Link
SecurityReason - IE6 CSS-Crash	Exploit, securityreason.com, text/html	SREASON 3295
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ie-scrollbarbasecolor-dos(13809)
SecurityFocus HOME Mailing List: BugTraq	Exploit, www.securityfocus.com, text/html	BUGTRAQ 20031022 IE6 CSS-Crash
Microsoft Internet Explorer Scrollbar-Base-Color Partial Denial Of Service Vulnerability	Exploit, cve.report (archive), text/html	BID 8874

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→

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