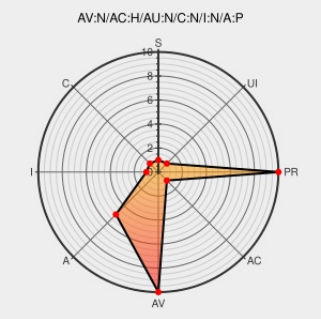
CVE-2005-1790

Published on: 06/01/2005 12:00:00 AM UTC

Last Modified on: 07/23/2021 03:04:00 PM UTC

CVE-2005-1790

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



Certain versions of Ie from Microsoft contain the following vulnerability:

Microsoft Internet Explorer 6 SP2 6.0.2900.2180 and 6.0.2800.1106, and earlier versions, allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a Javascript BODY onload event that calls the window function, aka "Mismatched Document Object Model Objects Memory Corruption Vulnerability."

CVE-2005-1790 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

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

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1303
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2867
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1299
	support.avaya.com application/pdf	CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-234.pdf
Computer Terrorism (UK) :: Security Advisory	www.computerterrorism.com text/html	MISC www.computerterrorism.com/research/ie/ct21-11-2005

Secunia - Advisories - Microsoft Internet Explorer "window()" Arbitrary Code Execution Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 15546
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:722
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2509
Nortel Centrex IP Client Manager Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18311
Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability	cve.report (archive) text/html	BID 13799
Microsoft Security Bulletin MS05-054 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS05-054
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1508
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051121 Computer Terrorism Security Advisory (Reclassification) - Microsoft Internet Explorer JavaScript Window() Vulnerability
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1091
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1489
Nortel: Technical Support	web.archive.org text/html Inactive Link Not Archived	MISC www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=375420
US-CERT Technical Cyber Security Alert TA05-347A -- Microsoft Internet Explorer Vulnerabilities	US Government Resource www.us-cert.gov text/html	CERT TA05-347A
US-CERT Vulnerability Note VU#887861	US Government Resource www.kb.cert.org text/html	CERT-VN VU#887861
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2909
SecurityTracker.com Archives - Microsoft Internet Explorer Bug in Processing Mismatched Document Object Model Objects May Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1015251
'Re: Microsoft Internet Explorer - Crash on JavaScript "window()"-calling (05/28/2005)' - MARC	marc.info text/html	BUGTRAQ 20050530 Re: Microsoft Internet Explorer - Crash on JavaScript "window()"-calling (05/28/2005)
Secunia - Advisories - Avaya Products Microsoft Windows Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 18064
'Microsoft Internet Explorer - Crash on JavaScript "window()"-calling (05/28/2005)' - MARC	marc.info text/html	BUGTRAQ 20050528 Microsoft Internet Explorer - Crash on JavaScript "window()"-calling (05/28/2005)

Secunia - Advisories - Microsoft Internet Explorer Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 15368

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	6.0.2800.1106	All	All	All
Application	Microsoft	Ie	6.0.2900.2180	All	All	All
Application	Microsoft	Ie	6.0.2800.1106	All	All	All
Application	Microsoft	Ie	6.0.2900.2180	All	All	All
Application	Microsoft	Internet Explorer	6.0.2800.1106	All	All	All
Application	Microsoft	Internet Explorer	6.0.2900.2180	All	All	All

cpe:2.3:a:microsoft:ie:6.0.2800.1106:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0.2900.2180:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0.2800.1106:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0.2900.2180:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:6.0.2800.1106:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:6.0.2900.2180:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→