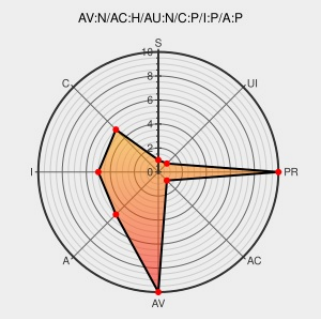
CVE-2005-2829

Published on: 12/14/2005 12:00:00 AM UTC

Last Modified on: 07/23/2021 12:55:00 PM UTC

CVE-2005-2829

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



Certain versions of Ie from Microsoft contain the following vulnerability:

Multiple design errors in Microsoft Internet Explorer 5.01, 5.5, and 6 allow user-assisted attackers to execute arbitrary code by (1) overlaying a malicious new window above a file download box, then (2) using a keyboard shortcut and delaying the display of the file download box until the user hits a shortcut that activates the "Run" button, aka "File Download Dialog Box Manipulation Vulnerability."

CVE-2005-2829 has been assigned by secure@microsoft.com 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ie-dialog-box-code-execution(23448)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1458
'[Full-disclosure] Secunia Research: Microsoft Internet Explorer' - MARC	marc.info text/html	FULLDISC 20051213 Secunia Research: Microsoft Internet Explorer Keyboard Shortcut Processing Vulnerability
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2867
Repository / Oval Repository	oval.cisecurity.org	OVAL oval:org.mitre.oval:def:1505

	text/html	
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1507
	support.avaya.com application/pdf	CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-234.pdf
Microsoft Internet Explorer Dialog Manipulation Vulnerability	Patch cve.report (archive) text/html	BID 15823
Nortel Centrex IP Client Manager Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 18311
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1209
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:1340
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
About Secunia Research | Flexera	Patch Vendor Advisory secunia.com Depreciated Link text/plain	MISC secunia.com/secunia_research/2005-21/advisory
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1490
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2909
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051213 Secunia Research: Internet Explorer Suppressed "Download Dialog"Vulnerability
Secunia - Advisories - Avaya Products Microsoft Windows Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 18064
Secunia - Advisories - Microsoft Internet Explorer Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 15368
SecurityTracker.com Archives - Microsoft Windows Internet Explorer May Let Remote Users Obfuscate the Download Dialog Box	securitytracker.com text/html	SECTRACK 1015349
About Secunia Research | Flexera	Patch Vendor Advisory secunia.com Depreciated Link text/plain	MISC secunia.com/secunia_research/2005-7/advisory/
SecurityReason - Internet Explorer Suppressed "Download Dialog"Vulnerability	securityreason.com text/html	SREASON 254

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	5.0.1	sp4	All	All
Application	Microsoft	Ie	5.5	sp2	All	All
Application	Microsoft	Ie	6.0	All	All	All
Application	Microsoft	Ie	6.0	sp1	All	All
Application	Microsoft	Ie	5.0.1	sp4	All	All
Application	Microsoft	Ie	5.5	sp2	All	All
Application	Microsoft	Ie	6.0	All	All	All
Application	Microsoft	Ie	6.0	sp1	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp4	All	All
Application	Microsoft	Internet Explorer	5.5	sp2	All	All
Application	Microsoft	Internet Explorer	6.0	All	All	All

cpe:2.3:a:microsoft:ie:5.0.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:5.5:sp2:*:*:*:*:*:*:

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

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

cpe:2.3:a:microsoft:ie:5.0.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:5.5:sp2:*:*:*:*:*:*:

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

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

cpe:2.3:a:microsoft:internet_explorer:5.0.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:5.5:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→