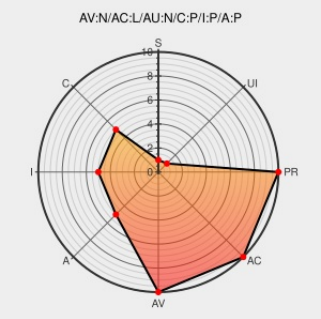
CVE-2005-3591

Published on: 11/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-3591

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



Certain versions of Flash Player from Macromedia contain the following vulnerability:

Macromedia Flash plugin (1) Flash.ocx 7.0.19.0 (Windows) and earlier and (2) libflashplayer.so before 7.0.25.0 (Unix) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via parameters to the ActionDefineFunction ActionScript call in a SWF file, which causes an improper memory access condition, a different vulnerability than CVE-2005-2628.

CVE-2005-3591 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Macromedia - MPSB05-07 : Flash Player 7 Improper Memory Access Vulnerability	Vendor Advisory, www.macromedia.com, text/xml	CONFIRM www.macromedia.com/devnet/security/security_zone/mpsb05-07.html
SecurityReason - Macromedia Flash Player Improper Memory Access Vulnerability	securityreason.com, text/html	SREASON 149
Secunia - Advisories - Gentoo update for netscape-flash	Vendor Advisory, web.archive.org, text/html	SECUNIA 17738
Macromedia Flash ActionDefineFunction Memory Access Vulnerability	Exploit, Patch, cve.report (archive)	BID 15334

	text/html	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2005-2317
Secunia - Advisories - SUSE Updates for Multiple Packages	Vendor Advisory web.archive.org text/html	SECUNIA 17626
Secunia - Advisories - Internet Explorer Macromedia Flash Player SWF Arbitrary Code Execution	Vendor Advisory web.archive.org text/html	SECUNIA 17481
404 - Page not found! - SEC Consult	Exploit Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.sec-consult.com/226.html
Secunia - Advisories - Macromedia Flash Player SWF File Handling Arbitrary Code Execution	Patch Vendor Advisory web.archive.org text/html	SECUNIA 17430
Secunia - Advisories - Opera Macromedia Flash Player SWF Arbitrary Code Execution	Vendor Advisory web.archive.org text/html	SECUNIA 17437
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF flash-actiondefinefunction-doaction-bo(23022)
'SEC Consult SA-20051107-1 :: Macromedia Flash Player ActionDefineFunction' - MARC	marc.info text/html	BUGTRAQ 20051107 SEC Consult SA-20051107-1 :: Macromedia Flash Player ActionDefineFunction
Microsoft Security Advisory (910550): Macromedia Security Bulletin: MPSB05-07 Flash Player 7 Improper Memory Access Vulnerability	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MSKB Q910550

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Macromedia	Flash Player	6.0	All	All	All
Application	Macromedia	Flash Player	6.0.29.0	All	All	All
Application	Macromedia	Flash Player	6.0.40.0	All	All	All
Application	Macromedia	Flash Player	6.0.47.0	All	All	All
Application	Macromedia	Flash Player	6.0.65.0	All	All	All
Application	Macromedia	Flash Player	6.0.79.0	All	All	All

Application	Macromedia	Flash Player	7.0.19.0	All	All	All
Application	Macromedia	Flash Player	7.0_r19	All	All	All
Application	Macromedia	Flash Player	6.0	All	All	All
Application	Macromedia	Flash Player	6.0.29.0	All	All	All
Application	Macromedia	Flash Player	6.0.40.0	All	All	All
Application	Macromedia	Flash Player	6.0.47.0	All	All	All
Application	Macromedia	Flash Player	6.0.65.0	All	All	All
Application	Macromedia	Flash Player	6.0.79.0	All	All	All
Application	Macromedia	Flash Player	7.0.19.0	All	All	All
Application	Macromedia	Flash Player	7.0_r19	All	All	All

cpe:2.3:a:macromedia:flash_player:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.29.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.40.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.47.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.65.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.79.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:7.0.19.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:7.0_r19:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.29.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.40.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.47.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.65.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:6.0.79.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:7.0.19.0:*:*:*:*:*:*:*:

cpe:2.3:a:macromedia:flash_player:7.0_r19:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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