



CVE-2005-4216

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2005-4216
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-14 11:03:00 UTC
Updated	2017-07-20 01:29:00 UTC
Description	The Administration Service (FMSAdmin.exe) in Macromedia Flash Media Server 2.0 r1145 allows remote attackers to caus

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Macromedia	Flash Media Server	2.0	All	developer	All
Application	Macromedia	Flash Media Server	2.0	All	edge	All
Application	Macromedia	Flash Media Server	2.0	All	origin	All
Application	Macromedia	Flash Media Server	2.0	All	professional	All
Application	Macromedia	Flash Media Server	2.0_r1145	All	All	All
Application	Macromedia	Flash Media Server	2.0	All	developer	All
Application	Macromedia	Flash Media Server	2.0	All	edge	All
Application	Macromedia	Flash Media Server	2.0	All	origin	All
Application	Macromedia	Flash Media Server	2.0	All	professional	All
Application	Macromedia	Flash Media Server	2.0_r1145	All	All	All

References

Reference	Source	Link
Secunia - Advisories - Macromedia Flash Media Server Administration Service Denial of Service	SECUNIA	secunia.com
SecurityTracker.com Archives - Flash Media Server Lets Remote Users Deny Service	SECTRACK	securitytracker.com
IBM X-Force Exchange	XF	exchange.xforce.ibm
Ioannis	MISC	www.ipomonis.com

Macromedia Flash Media Server 2 Administration Service Remote Denial of Service Vulnerability	BID	www.securityfocus.com
Macromedia - MPSB05-11 : Administrator Interface Denial of Service Vulnerability in Flash Media Server	CONFIRM	www.macromedia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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