



CVE-2007-2500

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

Summary

CVE	CVE-2007-2500
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-04 00:19:00 UTC
Updated	2017-07-29 01:31:00 UTC
Description	server/parser/sprite_definition.cpp in GNU Gnash (aka GNU Flash Player) 0.7.2 allows remote attackers to execute arbitrar

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Flash Player	All	All	All	All

References

Reference	Source	Link
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
37273	OSVDB	osvdb.org
Gnash - The GNU Flash player - Bugs: bug #19774, URGENT: Out of bounds memory... [Savannah]	MISC	savannah.gnu.org
Gnash DefineSprite Tag Remote Code Execution Vulnerability	BID	www.securityfocus.com
Webmail - OVH	VUPEN	www.vupen.com
Security Announcement	SUSE	www.novell.com
Gnash DEFINESPRITE Tag Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.co
IBM X-Force Exchange	XF	exchange.xforce.ibmcl
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)