



CVE-2007-1473

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

Summary

CVE	CVE-2007-1473
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-16 21:19:00 UTC
Updated	2018-10-16 16:38:00 UTC
Description	Cross-site scripting (XSS) vulnerability in framework/NLS/NLS.php in Horde Framework before 3.1.4 RC1, when the login p

Risk And Classification

Problem Types: NVD-CWE-Other


NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Horde	Horde Application Framework	1.2.0	All	All	All
Application	Horde	Horde Application Framework	1.2.1	All	All	All
Application	Horde	Horde Application Framework	1.2.2	All	All	All
Application	Horde	Horde Application Framework	1.2.3	All	All	All
Application	Horde	Horde Application Framework	1.2.4	All	All	All
Application	Horde	Horde Application Framework	1.2.5	All	All	All
Application	Horde	Horde Application Framework	1.2.6	All	All	All
Application	Horde	Horde Application Framework	1.2.7	All	All	All
Application	Horde	Horde Application Framework	1.2.8	All	All	All
Application	Horde	Horde Application Framework	1.3.3	All	All	All
Application	Horde	Horde Application Framework	1.3.4	All	All	All
Application	Horde	Horde Application Framework	2.0	All	All	All
Application	Horde	Horde Application Framework	2.1	All	All	All
Application	Horde	Horde Application Framework	2.2	All	All	All
Application	Horde	Horde Application Framework	2.2.1	All	All	All
Application	Horde	Horde Application Framework	2.2.3	All	All	All
Application	Horde	Horde Application Framework	2.2.4	All	All	All

Application	Horde	Horde Application Framework	2.2.3	All	All	All
Application	Horde	Horde Application Framework	2.2.4	All	All	All
Application	Horde	Horde Application Framework	2.2.5	All	All	All
Application	Horde	Horde Application Framework	2.2.6	All	All	All
Application	Horde	Horde Application Framework	2.2.7	All	All	All
Application	Horde	Horde Application Framework	2.2.8	All	All	All
Application	Horde	Horde Application Framework	2.2.9	All	All	All
Application	Horde	Horde Application Framework	3.0.0	All	All	All
Application	Horde	Horde Application Framework	3.0.1	All	All	All
Application	Horde	Horde Application Framework	3.0.10	All	All	All
Application	Horde	Horde Application Framework	3.0.2	All	All	All
Application	Horde	Horde Application Framework	3.0.3	All	All	All
Application	Horde	Horde Application Framework	3.0.4	All	All	All
Application	Horde	Horde Application Framework	3.0.5	All	All	All
Application	Horde	Horde Application Framework	3.0.6	All	All	All
Application	Horde	Horde Application Framework	3.0.7	All	All	All
Application	Horde	Horde Application Framework	3.0.8	All	All	All
Application	Horde	Horde Application Framework	3.0.9	All	All	All
Application	Horde	Horde Application Framework	3.1.0	All	All	All
Application	Horde	Horde Application Framework	3.1.1	All	All	All
Application	Horde	Horde Application Framework	3.1.2	All	All	All
Application	Horde	Horde Application Framework	3.1.3	All	All	All

References

Reference	Source
33084	OSVD
IBM X-Force Exchange	XF
SUSE Update for Multiple Packages - Advisories - Secunia	SECUL
Debian update for horde3 - Advisories - Secunia	SECUL
Horde Framework Login.PHP Cross-Site Scripting Vulnerability	BID
Horde Language Selection Cross-Site Scripting Vulnerability - Advisories - Secunia	SECUL
SecurityReason - Horde 3.1.4 (RC1) fixes XSS issue	SREA
Security Announcement	SUSE
[announce] Horde 3.1.4 (final)	MLIS
SecurityFocus	BUGT
Webmail - OVH	VUPE

Debian -- Security Information -- DSA-1406-1 horde3	DEBI/
SecurityTracker.com Archives - Horde Application Framework Input Validation Flaw in 'NLS.php' Permits Cross-Site Scripting Attacks	SECT
CVE Program record	CVE.C
NVD vulnerability detail	NVD
	
<p>No vendor comments have been submitted for this CVE.</p>	
<p>There are currently no legacy QID mappings associated with this CVE.</p>	

© [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](#)