



CVE-2002-0217

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

Summary

CVE	CVE-2002-0217
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-05-16 04:00:00 UTC
Updated	2008-09-11 00:00:00 UTC
Description	Cross-site scripting (CSS) vulnerabilities in the Private Message System for XOOPS 1.0 RC1 allow remote attackers to exe

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xoops	Xoops	1.0_rc1	All	All	All
Application	Xoops	Xoops	1.0_rc1	All	All	All

References

Reference	Source	Link
20020129 Xoops Private Message System Script injection	BUGTRAQ	online.securi
ISS X-Force Database: xoops-private-message-css (8025): XOOPS Private Message System cross-site scripting	XF	www.iss.net
ISS X-Force Database: xoops-pmlite-image-css (8030): XOOPS pmlite.php cross-site scripting	XF	www.iss.net
Xoops Private Message System Cross-Agent Scripting Vulnerability	BID	www.securit
Xoops Private Message Box Cross-Agent Scripting Vulnerability	BID	www.securit
CVE Program record	CVE.ORG	www.cve.or
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](#)