[DSECRG−08−041] Stored XSS Vulnerability in Xoops 2.3.x

Source: http://www.derkeiler.com/Mailing−Lists/securityfocus/bugtraq/2008−12/msg00074.html

- *From*: "Digital Security Research Group [DSecRG]" <research@xxxxxxx>
- *Date*: Mon, 8 Dec 2008 15:21:47 +0300

Digital Security Research Group [DSecRG] Advisory #DSECRG−08−041

Application: XOOPS
Versions Affected: 2.3.1, 2.3.2a
Vendor URL: http://www.xoops.org/
Bug: Stored XSS
Exploits: YES
Reported: 10.11.2008
Vendor response: 10.11.2008
Solution: YES
Date of Public Advisory: 08.12.2008
Authors: Digital Security Research Group [DSecRG] (research [at] dsec [dot] ru)

Description
****

XOOPS has Stored XSS vulnerability.

Details
****

Vulnerability found in script pmlite.php

User can inject script into private message using BBCode post parameter [url].

Example:

[url=" STYLE="test:expression(alert('DSecRG XSS'))]DSecRG XSS[/url]

Solution

****

Vendor fixed this flaw on 07.12.2008.

XOOPS 2.3.2b Security Release can be download from Sourceforge repository:

https://sourceforge.net/project/showfiles.php?group_id=41586&package_id=153583&release_id=643845

Release notes:

http://www.xoops.org/modules/news/article.php?storyid=4563

About
*****

Digital Security is leading IT security company in Russia, providing information security consulting, audit and penetration testing services, risk analysis and ISMS−related services and certification for ISO/IEC 27001:2005 and PCI DSS standards. Digital Security Research Group focuses on web application and database security problems with vulnerability reports, advisories and whitepapers posted regularly on our website.

Contact: research [at] dsec [dot] ru
http://www.dsec.ru (in Russian)