



CVE-2009-3666

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

Summary

CVE	CVE-2009-3666
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-11 22:30:00 UTC
Updated	2018-10-10 19:47:00 UTC
Description	Cross-site scripting (XSS) vulnerability in index.php in Nullam Blog 0.1.2 allows remote attackers to inject arbitrary web scri

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nullam	Nullam Blog	0.1.2	All	All	All
Application	Nullam	Nullam Blog	0.1.2	All	All	All

References

Reference	Source	Link
Nullam Blog Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secuni
SecurityFocus	BUGTRAQ	www.s
nullam blog 0.1.2 - Local File Inclusion / File Disclosure / SQL Injection / Cross-Site Scripting - PHP webapps Exploit	EXPLOIT-DB	www.e
57921	OSVDB	www.c
IBM X-Force Exchange	XF	exchar
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#)