



CVE-2012-5297

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

Summary

CVE	CVE-2012-5297
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-04 17:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	SQL injection vulnerability in edit.asp in Mavili Guestbook, as released in November 2007, allows remote attackers to execute

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mavili Guestbook Project	Mavili Guestbook	-	All	All	All
Application	Mavili Guestbook Project	Mavili Guestbook	-	All	All	All

References

Reference	Source	Link
20120103 mavili guestbook - SQL Injection and XSS Vulnerabilities	BUGTRAQ	arc
IBM X-Force Exchange	XF	exc
Mavili Guestbook Multiple Security Vulnerabilities	BID	ww
Issue 1 - maviliguestbook - Multiple security vulnerabilities announced - asp (vbscript) guestbook - Google Project Hosting	MISC	coc
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

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](#)