



CVE-2008-5926

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

Summary

CVE	CVE-2008-5926
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-21 18:30:00 UTC
Updated	2017-09-29 01:32:00 UTC
Description	Multiple SQL injection vulnerabilities in login.asp in ASP-DEv Internal E-Mail System allow remote attackers to execute arbitrary

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asp-dev	Internal E-mail System	All	All	All	All
Application	Asp-dev	Internal E-mail System	All	All	All	All

References

Reference	Source
32808	BID
ASP-DEV Internal E-Mail System - Authentication Bypass - ASP webapps Exploit	EXPL
ASP-DEV Internal E-Mail System "login" and "password" SQL Injection - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
SecurityReason - ASP-DEV Internal E-Mail System (Auth Bypass) SQL Injection Vuln	SREA
CVE Program record	CVE
NVD vulnerability detail	NVD

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](#)