



CVE-2006-4295

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

Summary

CVE	CVE-2006-4295
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-23 01:04:00 UTC
Updated	2008-09-05 21:09:00 UTC
Description	Cross-site scripting (XSS) vulnerability in ascan_6.asp in Panda ActiveScan 5.53.00 allows remote attackers to inject arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Panda	Panda Activescan	5.53.00	All	All	All
Application	Panda	Panda Activescan	5.53.00	All	All	All

References

Reference	Source	Link
Panda ActiveScan Input Validation Hole in 'email' Parameter Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	securitytr
Lostmon's Blogger: Panda ActiveScan XSS vulnerability	MISC	lostmon.l
RETIRED: Panda ActiveScan Ascan_6.ASP ActiveX Control Cross-Site Scripting Vulnerability	BID	www.sec
29147	OSVDB	www.osv
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)