



CVE-2010-3926

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

Summary

CVE	CVE-2010-3926
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-12 01:00:00 UTC
Updated	2017-08-17 01:33:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in Shop.cgi in SGX-SP Final before 11.00 and SGX-SP Final NE before 11

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wb-i	Sgx-sp Final	All	All	All	All
Application	Wb-i	Sgx-sp Final Ne	All	All	All	All

References

Reference	Source	Link
wb-i.net/soft1.HTML	CONFIRM	wb-i.net
JVN#86347943: SGX-SP Final および SGX-SP Final NE におけるクロスサイトスクリプティングの脆弱性	JVN	jvn.jp
JVNDB-2011-000002	JVNDB	jvndb.jvn.jp
70410	OSVDB	osvdb.org
SGX-SP Final Multiple Cross-Site Scripting Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibm
SGX-SP Final 'shop.cgi' Multiple Cross Site Scripting Vulnerabilities	BID	www.securityfocus
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)