



CVE-2014-0681

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

Summary

CVE	CVE-2014-0681
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-29 18:34:00 UTC
Updated	2018-01-03 02:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Cisco Identity Services Engine (ISE) 1.2 patch 2 and earlier allows remote attackers

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine Software	All	All	All	All

References

Reference	Source
Cisco Identity Services Engine Report Page HTML Injection Vulnerability	BID
Cisco Identity Services Engine Input Validation Flaw in Report Output Pages Permits Cross-Site Scripting Attacks - SecurityTracker	SECTR
Security Advisory SA56714 - Cisco Identity Service Engine (ISE) Reports Pages Cross-Site Scripting Vulnerability - Secunia	SECUN
Alert Details - Security Center - Cisco Systems	CONFII
Cisco Security Notice: Cisco Identity Services Engine Reports Output Cross-Site Scripting Vulnerability	CISCO
102589	OSVDE
CVE Program record	CVE.OI
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](#)