



CVE-2014-5172

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

Summary

CVE	CVE-2014-5172
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-31 14:55:00 UTC
Updated	2018-10-09 19:50:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the XS Administration Tools in SAP HANA allow remote attackers to inject

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Hana	-	All	All	All
Application	Sap	Hana	-	All	All	All

References

Reference	Source
SAP HANA Extended Application Services Multiple Cross Site Scripting Vulnerabilities	BID
Onapsis - Register	MIS
Acknowledgments to Security Researchers SCN	CC
IBM X-Force Exchange	XF
SecurityFocus	BU
Full Disclosure: [Onapsis Security Advisory 2014-025] Multiple Cross Site Scripting Vulnerabilities in SAP HANA XS Administration Tool	FU
Security Advisory SA59634 - SAP HANA XS Administration Tool Cross-Site Scripting Vulnerabilities - Secunia	SE
service.sap.com/sap/support/notes/1993349	CC
SAP HANA XS Administration Tool Cross Site Scripting ~ Packet Storm	MIS
CVE Program record	CV
NVD vulnerability detail	NV

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](#)