



CVE-2014-8314

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

Summary

CVE	CVE-2014-8314
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-16 19:55:00 UTC
Updated	2018-10-09 19:53:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in SAP HANA Developer Edition Revision 70 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	All
Application	Sap	Hana	All	All	All	All

References

Reference	Source	Link
Acknowledgments to Security Researchers - Previ... SCN	CONFIRM	scn.s
Full Disclosure: [Onapsis Security Advisory 2014-027] SAP HANA Multiple Reflected Cross Site Scripting Vulnerabilities	FULLDISC	seclis
SAP HANA Reflective Cross Site Scripting ≈ Packet Storm	MISC	packe
Malformed Request	BID	www.
Page Not Found Onapsis	MISC	www.
service.sap.com/sap/support/notes/2009696	CONFIRM	servi
IBM X-Force Exchange	XF	excha
SecurityFocus	BUGTRAQ	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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](#)