



CVE-2016-6150

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

Summary

CVE	CVE-2016-6150
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-05 14:59:00 UTC
Updated	2016-11-28 20:30:00 UTC
Description	The multi-tenant database container feature in SAP HANA does not properly encrypt communications, which allows remote

Risk And Classification

Problem Types: CWE-284

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	Link
Malformed Request	BID	www.securityfocus.co
Full Disclosure: Onapsis Security Advisory ONAPSIS-2016-040: SAP HANA potential wrong encryption	FULLDISC	seclists.org
SAP HANA Potential Wrong Encryption Onapsis	MISC	www.onapsis.com
SAP HANA DB Encryption Issue ≈ Packet Storm	MISC	packetstormsecurity.c
Page not found - Layer Seven Security	MISC	layersevensecurity.co
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](#)