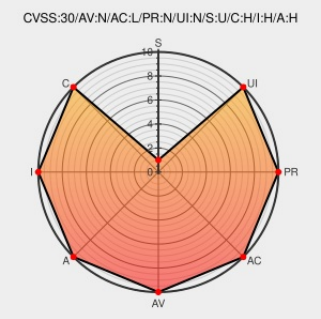
CVE-2016-1928

Published on: 01/20/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1928

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Hana from Sap contain the following vulnerability:

Buffer overflow in the XS engine (hdbxsengine) in SAP HANA allows remote attackers to cause a denial of service or execute arbitrary code via a crafted HTTP request, related to JSON, aka SAP Security Note 2241978.

CVE-2016-1928 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160427 Re: [ERPSCAN-16-005] SAP HANA hdbxsengine JSON - DoS vulnerability
SAP Note Security Analysis - January 2016	erpscan.io text/html	MISC erpscan.io/press-center/blog/sap-security-notes-january-2016-review/

[ERPSCAN-16-005] SAP HANA hdbxsengine JSON - DoS	erpscan.io text/html	MISC erpscan.io/advisories/erpscan-16-005-sap-hana-hdbxsengine-json-dos/
Full Disclosure: [ERPSCAN-16-005] SAP HANA hdbxsengine JSON – DoS vulnerability	seclists.org text/html	FULLDISC 20160420 [ERPSCAN-16-005] SAP HANA hdbxsengine JSON - DoS vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:sap:hana:-:*:*:*:*:*:*:*:

cpe:2.3:a:sap:hana:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→