



CVE-2020-26834

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-26834 |
| State | PUBLIC |
| Assigner | cna@sap.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-12-09 17:15:00 UTC |
| Updated | 2020-12-10 21:38:00 UTC |
| Description | SAP HANA Database, version - 2.0, does not correctly validate the username when performing SAML bearer token-based |

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------|-------------------------------|---------|--------|---------|----------|
| Application | Sap | Hana Database | 2.00 | All | All | All |
| Application | Sap | Hana Database | 2.00 | All | All | All |

References

| Reference | Source | Link |
|--|---------|---|
| launchpad.support.sap.com | MISC | launchpad.support.sap.com |
| SAP Security Patch Day – December 2020 - Product Security Response at SAP - Community Wiki | MISC | wiki.scn.sap.com |
| 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.

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