



# CVE-2020-26838

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

## Summary

|                        |                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2020-26838                                                                                                     |
| <b>State</b>           | PUBLIC                                                                                                             |
| <b>Assigner</b>        | cna@sap.com                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                       |
| <b>Published</b>       | 2020-12-09 17:15:00 UTC                                                                                            |
| <b>Updated</b>         | 2020-12-10 21:01:00 UTC                                                                                            |
| <b>Description</b>     | SAP Business Warehouse, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 782, and SAP BW4HANA, ve |

## Risk And Classification

### Problem Types: CWE-78

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product                            | Version | Update | Edition | Language |
|-------------|---------------------|------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 700     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 701     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 702     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 731     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 740     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 750     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 751     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 752     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 753     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 754     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 755     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 782     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 700     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 701     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 702     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 731     | All    | All     | All      |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 740     | All    | All     | All      |

|             |                     |                                    |     |     |     |     |
|-------------|---------------------|------------------------------------|-----|-----|-----|-----|
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 750 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 751 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 752 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 753 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 754 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 755 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Business Warehouse</a> | 782 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Bw/4hana</a>           | 100 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Bw/4hana</a>           | 200 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Bw/4hana</a>           | 100 | All | All | All |
| Application | <a href="#">Sap</a> | <a href="#">Bw/4hana</a>           | 200 | All | All | All |

| References                                                                                 |         |                                           |
|--------------------------------------------------------------------------------------------|---------|-------------------------------------------|
| Reference                                                                                  | Source  | Link                                      |
| SAP Security Patch Day – December 2020 - Product Security Response at SAP - Community Wiki | MISC    | <a href="#">wiki.scn.sap.com</a>          |
| launchpad.support.sap.com                                                                  | MISC    | <a href="#">launchpad.support.sap.com</a> |
| CVE Program record                                                                         | CVE.ORG | <a href="#">www.cve.org</a>               |
| NVD vulnerability detail                                                                   | NVD     | <a href="#">nvd.nist.gov</a>              |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.