



CVE-2014-8312

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

Summary

CVE	CVE-2014-8312
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-16 19:55:00 UTC
Updated	2022-10-06 15:20:00 UTC
Description	Business Warehouse (BW) in SAP Netweaver AS ABAP 7.31 allows remote authenticated users to obtain sensitive informa

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Netweaver Abap	7.31	All	All	All
Application	Sap	Netweaver Abap	7.31	All	All	All

References

Reference
SAP NetWeaver Business Warehouse Access Bypass Vulnerability
Security Advisory SA61101 - SAP NetWeaver Business Warehouse "RSDU_CCMS_GET_PROFILE_PARAM" Security Bypass Se
Acknowledgments to Security Researchers SCN
Full Disclosure: [Onapsis Security Advisory 2014-033] SAP Business Warehouse Missing Authorization Check
Page Not Found Onapsis
service.sap.com/sap/support/notes/1967780
SAP Business Warehouse Missing Authorization Check ≈ Packet Storm
SecurityFocus
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

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](#)