CVE-2006-0732

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0732
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-16 11:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Directory traversal vulnerability in SAP Business Connector (BC) 4.6 and 4.7 allows remote attackers to read or delete arbit

Risk And Classification

Primary CVSS: v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:N

EPSS: 0.030810000 probability, percentile 0.867870000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Sap	Business Connector	4.6	All	All	All
Application	Sap	Business Connector	4.7	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sour
SAP Business Connector Arbitrary File Access and Spoofing - Advisories - Secunia	af854
SecurityTracker.com Archives - SAP Business Connector Bugs Let Remote Users View or Delete Files and Conduct Phishing Attacks	af854
www.cybsec.com/vuln/CYBSEC_Security_Pre-Advisory_Arbitrary_File_Read_or_Dele...	af854
SAP sapdba Command for Informix Environment Variable Bug Lets Local Users Gain Elevated Privileges - SecurityTracker	af854
SAP Business Connector Lets Remote Authenticated Users View and Delete Files - SecurityTracker	af854
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
www.cybsec.com/vuln/CYBSEC_Security_Advisory_Arbitrary_File_Read_or_Delete_i...	af854
SecurityFocus	af854
SecurityFocus	af854
SAP Business Connector Remote Arbitrary File Access And Deletion Vulnerability	af854
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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