



# OS Command Injection vulnerability in SAP NetWeaver Application Server for ABAP and ABAP Platform

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

## Summary

<b>CVE</b>	CVE-2026-40135
<b>State</b>	PUBLISHED
<b>Assigner</b>	sap
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 03:16:12 UTC
<b>Updated</b>	2026-05-12 03:16:12 UTC
<b>Description</b>	An OS Command Injection vulnerability exists in the SAP NetWeaver Application Server for ABAP and ABAP Platform that

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from cna@sap.com

**CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H**

**Problem Types:** CWE-77 | CWE-77 CWE-77: Improper Neutralization of Special Elements used in a Command

Version	Source	Type	Score	Severity	Vector
3.1	cna@sap.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**High**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**None**

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 700	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 701	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 702	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 731	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 740	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 750	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 751	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 752	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 753	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 754	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 755	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 756	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 757	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 758	Not specified
CNA	SAP SE	SAP NetWeaver Application Server For ABAP And ABAP Platform	affected SAP_BASIS 816	Not specified

### References

Reference	Source	Link	Tags
<a href="url.sap/sapsecuritypatchday">url.sap/sapsecuritypatchday</a>	cna@sap.com	<a href="url.sap">url.sap</a>	
<a href="me.sap.com/notes/3730019">me.sap.com/notes/3730019</a>	cna@sap.com	<a href="me.sap.com">me.sap.com</a>	
CVE Program record	CVE.ORG	<a href="www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)