



An Láirionad Náisiúnta  
Cibearshlándála  
National Cyber  
Security Centre

NCSC #2607140228

# NCSC Advisory

## Critical Memory Corruption Vulnerability - SAP NetWeaver Application Server ABAP CVE-2026-44747

14th, July 2026

**STATUS: TLP:CLEAR**

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>.  
Please treat this document in accordance with the TLP assigned.



## Description

**CVE ID:** CVE-2026-44747

**Published:** 2026-07-14

**Vendor:** SAP\_SE

**Product:** SAP NetWeaver Application Server ABAP

**CVSS Score<sup>1</sup>:** 9.9

## Products Affected

| Product                               | Version        |
|---------------------------------------|----------------|
| SAP NetWeaver Application Server ABAP | KRNL64NUC 7.22 |
| SAP NetWeaver Application Server ABAP | 7.22EXT        |
| SAP NetWeaver Application Server ABAP | KRNL64UC 7.22  |
| SAP NetWeaver Application Server ABAP | 7.53           |
| SAP NetWeaver Application Server ABAP | KERNEL 7.22    |
| SAP NetWeaver Application Server ABAP | 7.53. 7.54     |
| SAP NetWeaver Application Server ABAP | 7.77           |
| SAP NetWeaver Application Server ABAP | 7.89           |
| SAP NetWeaver Application Server ABAP | 7.93           |
| SAP NetWeaver Application Server ABAP | 9.16           |
| SAP NetWeaver Application Server ABAP | 9.18           |
| SAP NetWeaver Application Server ABAP | 9.19           |
| SAP NetWeaver Application Server ABAP | 9.20           |

---

<sup>1</sup> <https://www.first.org/cvss/>



## Impact

SAP NetWeaver Application Server ABAP allows an authenticated attacker to leverage logical errors in memory management to cause a memory corruption that could lead to unauthorized data access, modification, or system unavailability. This has high impact on confidentiality, integrity, and availability of the application.,

**Common Weakness Enumeration (CWE)<sup>2</sup>: CWE-787: Out-of-bounds Write**

**Known Exploited Vulnerability (KEV) catalog<sup>3</sup>: No**

**Used by Ransomware Operators: N/A**

## Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from SAP.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-44747>
- <https://www.cve.org/CVERecord?id=CVE-2026-44747>
- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html>
- <https://me.sap.com/notes/3747367>
- <https://url.sap/sapsecuritypatchday>

---

<sup>2</sup> <https://cwe.mitre.org>

<sup>3</sup> <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>