An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605220210

NCSC Advisory

Critical Vulnerabilities exist in SAP S/4HANA and SAP Commerce Cloud Configuration

CVE-2026-34260, CVE-2026-34263

22nd, May 2026

STATUS: TLP:CLEAR

Description

CVE IDs: CVE-2026-34260, CVE-2026-34263

Published: 2026-05-12

Vendor: SAP_SE

Product: SAP S/4HANA (SAP Enterprise Search for ABAP), SAP Commerce cloud configuration

CVSS Score[1]: 9.6

CVE-2026-34260

Products Affected

Product	Version
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 751
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 752
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 753
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 754
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 755
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 756
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 757
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 758
SAP S/4HANA (SAP Enterprise Search for ABAP)	SAP_BASIS 816

[1] https://www.first.org/cvss/

Impact

SAP S/4HANA (SAP Enterprise Search for ABAP) contains a SQL injection vulnerability that allows an authenticated attacker to inject malicious SQL statements through user-controlled input. The application directly concatenates this malicious user input into SQL queries, which are then passed to the underlying database without proper validation or sanitization. Upon successful exploitation, an attacker may gain unauthorized access to sensitive database information and could potentially crash the application. This vulnerability has a high impact on the confidentiality and availability of the application, while integrity remains unaffected.

Common Weakness Enumeration (CWE)[2]: CWE-89: Improper Neutralization of Special Elements used in an SQL Command

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2026-34263

Products Affected

Product	Version
SAP Commerce cloud configuration	HY_COM 2205
SAP Commerce cloud configuration	COM_CLOUD 2211
SAP Commerce cloud configuration	2211-JDK21

Impact

Due to improper Spring Security configuration, SAP Commerce Cloud allows an unauthenticated user to perform malicious input injection, resulting in arbitrary server-side code execution, leading to high impact on Confidentiality, Integrity, and Availability of the application.

Common Weakness Enumeration (CWE)[4]: CWE-459: Incomplete Cleanup

Known Exploited Vulnerability (KEV) catalog[5]: 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_SE.

- https://nvd.nist.gov/vuln/detail/CVE-2026-34260
- https://www.cve.org/CVERecord?id=CVE-2026-34260
- https://nvd.nist.gov/vuln/detail/CVE-2026-34263
- https://www.cve.org/CVERecord?id=CVE-2026-34263
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html

[4] https://cwe.mitre.org
[5] https://www.cisa.gov/known-exploited-vulnerabilities-catalog