



An Lárionad Náisiúnta  
Cibearshlándála  
National Cyber  
Security Centre

NCSC #2602100215

# NCSC Advisory

SAP SE - SAP CRM and SAP S/4HANA (Scripting  
Editor)

CVE-2026-0488

10th, February 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-2026-0488

**Published:** 2026-02-10**Vendor:** SAP SE**Product:** SAP CRM and SAP S/4HANA (Scripting Editor)**CVSS Score<sup>1</sup>:** 9.9

## Products Affected

Product	Version
SAP CRM and SAP S/4HANA (Scripting Editor)	S4FND 102
SAP CRM and SAP S/4HANA (Scripting Editor)	103
SAP CRM and SAP S/4HANA (Scripting Editor)	104
SAP CRM and SAP S/4HANA (Scripting Editor)	105
SAP CRM and SAP S/4HANA (Scripting Editor)	106
SAP CRM and SAP S/4HANA (Scripting Editor)	107
SAP CRM and SAP S/4HANA (Scripting Editor)	108
SAP CRM and SAP S/4HANA (Scripting Editor)	109
SAP CRM and SAP S/4HANA (Scripting Editor)	SAP_ABA 700
SAP CRM and SAP S/4HANA (Scripting Editor)	WEBCUIF 700

---

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



SAP CRM and SAP S/4HANA (Scripting Editor)	701
SAP CRM and SAP S/4HANA (Scripting Editor)	730
SAP CRM and SAP S/4HANA (Scripting Editor)	731
SAP CRM and SAP S/4HANA (Scripting Editor)	746
SAP CRM and SAP S/4HANA (Scripting Editor)	747
SAP CRM and SAP S/4HANA (Scripting Editor)	748
SAP CRM and SAP S/4HANA (Scripting Editor)	800
SAP CRM and SAP S/4HANA (Scripting Editor)	801

## Impact

An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorised critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability.,

Common Weakness Enumeration (CWE)<sup>2</sup>: CWE-862: Missing Authorisation

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

Used by Ransomware Operators: N/A

---

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

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



## 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-2026-0488>
- <https://www.cve.org/CVERecord?id=CVE-2026-0488>
- <https://me.sap.com/notes/3697099>
- <https://url.sap/sapsecuritypatchday>