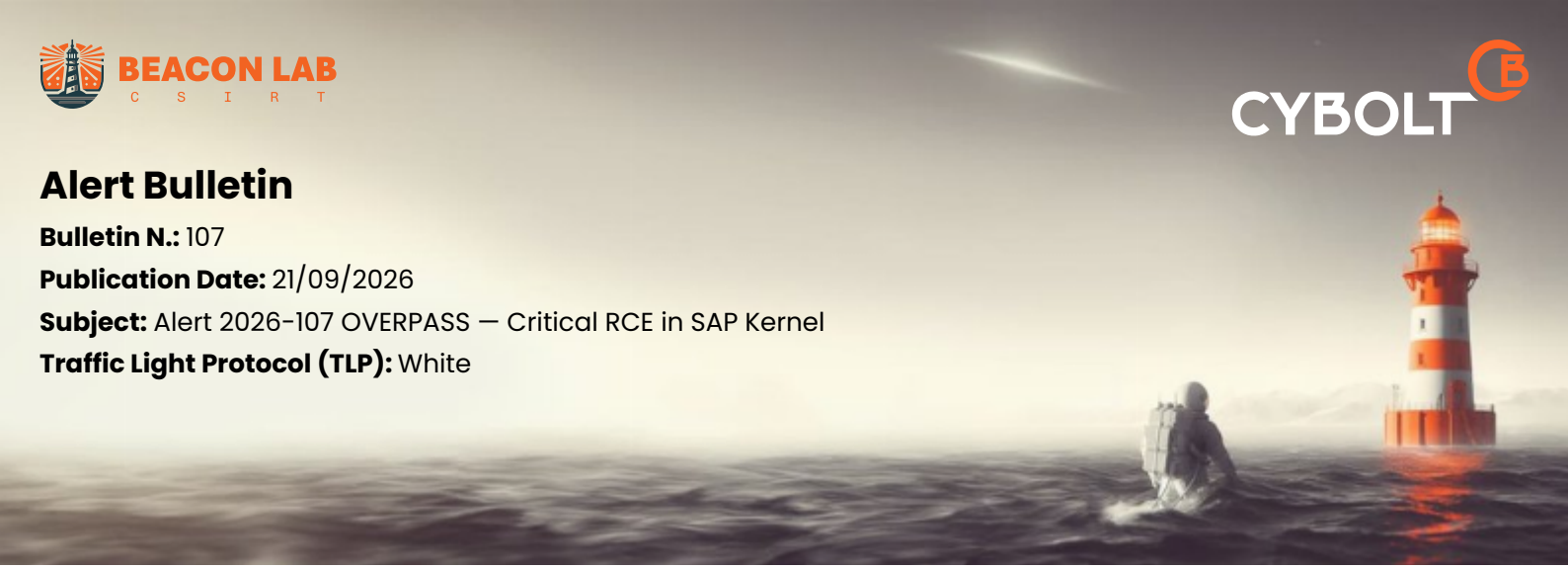

Alert Bulletin

Bulletin N.: 107
Publication Date: 21/09/2026
Subject: Alert 2026-107 OVERPASS — Critical RCE in SAP Kernel
Traffic Light Protocol (TLP): White

Affected product(s):

OVERPASS affects SAP software that uses the vulnerable **SAP Kernel** code, so the scope may include a significant proportion of SAP landscapes:

SAP product / component	Possible impact
SAP S/4HANA	Affected if using a vulnerable SAP Kernel version/patch level
SAP ERP / SAP Business Suite (ECC)	Affected if using a vulnerable SAP Kernel version/patch level
SAP NetWeaver Application Server ABAP	Affected if using a vulnerable SAP Kernel version/patch level
SAP Web Dispatcher	Affected if using a vulnerable SAP Kernel version/patch level
SAP BW/4HANA	Affected if using a vulnerable SAP Kernel version/patch level
SAP Enterprise Portal	Affected if using a vulnerable SAP Kernel version/patch level
SAP Process Integration / Process Orchestration (PI/PO)	Affected if using a vulnerable SAP Kernel version/patch level
SAP Solution Manager	Affected if using a vulnerable SAP Kernel version/patch level
Other products built on SAP NetWeaver Kernel	Potentially affected; validate against SAP Note 3747649

Definitive validation must be performed by comparing the kernel version and patch level of each system with **SAP Security Note 3747649.**

The scope criterion must be based on the kernel patch level, not solely on the product or web exposure. Old, development, QA, sandbox, DR, discontinued, or not published to the Internet systems may still be vulnerable through SAP GUI or RFC.

Description

A vulnerability identified as **CVE-2026-44756** and named **OVERPASS** was identified, a critical remote code execution (**RCE**) vulnerability in the SAP Kernel. The flaw has a **CVSS 10.0** score and allows an unauthenticated remote attacker to execute arbitrary operating system commands with the privileges of the SAP administrative account, which can lead to total compromise of the system, its business data, and trust relationships with other SAP environments.

CVE-2026-44756 (OVERPASS) is a vulnerability in the shared SAP Kernel code responsible for processing Extended Passport (EPP). EPP is a standard functionality used to correlate traces, calls, and messages in distributed SAP and non-SAP landscapes.

An attacker can send a specially crafted request with malformed EPP data to compromise the receiving process and execute operating system commands on the SAP host. The flaw is **pre-authentication**: EPP is processed when creating the session, so the vulnerable code is reached before SAP evaluates the user, password, authorizations, roles, account locks, or login policies.

Solution

The definitive solution is to apply the SAP Kernel patch indicated by **SAP Security Note 3747649**. A single kernel patch fixes the OVERPASS vulnerability in HTTP(S), SAP GUI, and RFC paths.

https://sapit-forme-prod.authentication.eu11.hana.ondemand.com/oauth/authorize?response_type=code&client_id=sb-forme-approuter!t1889&redirect_uri=https%3A%2F%2Fme.sap.com%2Flogin%2Fcallback

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1

Additional information:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1
- https://onapsis.com/blog/sap-overpass-remediation/
- https://me.sap.com/notes/3747649
- https://me.sap.com/notes/3776034
- https://me.sap.com/notes/3756304