

Boletín de alerta

Boletín Nro.: 107

Fecha de publicación: 21/09/2026

Tema: Alerta 2026-107 OVERPASS — RCE crítica en SAP Kernel

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

OVERPASS afecta a software SAP que utiliza el código vulnerable del **SAP Kernel**, por lo que el alcance puede incluir una proporción significativa de los paisajes SAP:

Producto / componente SAP	Posible afectación
SAP S/4HANA	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP ERP / SAP Business Suite (ECC)	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP NetWeaver Application Server ABAP	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP Web Dispatcher	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP BW/4HANA	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP Enterprise Portal	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP Process Integration / Process Orchestration (PI/PO)	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
SAP Solution Manager	Afectado si utiliza una versión/patch level vulnerable de SAP Kernel
Otros productos contruidos sobre SAP NetWeaver Kernel	Potencialmente afectados; validar contra SAP Note 3747649

La validación definitiva debe realizarse comparando la versión y el nivel de parche del kernel de cada sistema con la **SAP Security Note 3747649**.

El criterio de alcance debe basarse en el kernel patch level, no únicamente en el producto o en la exposición web. Sistemas antiguos, de desarrollo, QA, sandbox, DR, descontinuados o no publicados a Internet pueden seguir siendo vulnerables a través de SAP GUI o RFC.

Descripción

Se identificó una vulnerabilidad identificada como **CVE 2026 44756** y denominada como **OVERPASS**, una vulnerabilidad crítica de ejecución remota de código (**RCE**) en el SAP Kernel. La falla tiene una puntuación **CVSS 10.0** y permite a un atacante remoto no autenticado ejecutar comandos arbitrarios del sistema operativo con los privilegios de la cuenta administrativa de SAP, lo que puede conducir al compromiso total del sistema, sus datos de negocio y relaciones de confianza con otros entornos SAP.

CVE 2026 44756 (OVERPASS) es una vulnerabilidad en el código compartido del SAP Kernel responsable de procesar Extended Passport (EPP). EPP es una funcionalidad estándar empleada para correlacionar trazas, llamadas y mensajes en paisajes distribuidos SAP y no SAP.

Un atacante puede enviar una solicitud especialmente diseñada con datos EPP malformados para comprometer el proceso receptor y ejecutar comandos de sistema operativo en el host SAP. La falla es **preautenticación**: EPP se procesa al crear la sesión, por lo que el código vulnerable se alcanza antes de que SAP evalúe el usuario, la contraseña, las autorizaciones, los roles, los bloqueos de cuenta o las políticas de inicio de sesión.

Solución

La solución definitiva es aplicar el parche de SAP Kernel indicado por la **SAP Security Note 3747649**. Un único parche de kernel corrige la vulnerabilidad OVERPASS en las rutas HTTP(S), SAP GUI y RFC.

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

Información adicional:

- 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>