Boletín de alerta

Boletín Nro.: 25
Fecha de publicación: 12/03/2026
Tema: Alerta 2026-25 Vulnerabilidades críticas en SAP NetWeaver y SAP Supply Chain Management
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

SAP NetWeaver Enterprise Portal Administration

- EP-RUNTIME 7.50

SAP Supply Chain Management (SCM)

- SCMAPO 713
- SCMAPO 714
- SCM 700
- SCM 701
- SCM 702
- SCM 712
- S4CORE 102
- S4CORE 103
- S4CORE 104
- S4COREOP 105
- S4COREOP 106
- S4COREOP 107
- S4COREOP 108
- S4COREOP 109

Descripción

Recientemente, SAP publicó actualizaciones de seguridad que corrigen dos vulnerabilidades identificadas como **CVE-2026-27685 y CVE-2026-27689**, que afectan a componentes clave de **SAP NetWeaver Enterprise Portal Administration y SAP Supply Chain Management**. La más crítica de ellas, CVE-2026-27685, posee una puntuación **CVSS de 9.1 (crítica)** y se origina debido a un problema de deserialización insegura de datos no confiables (CWE-502) dentro del portal empresarial de SAP NetWeaver.

La vulnerabilidad CVE-2026-27685 ocurre cuando el sistema procesa objetos serializados provenientes de contenido cargado por usuarios privilegiados sin realizar validaciones adecuadas. La deserialización convierte datos serializados en objetos ejecutables dentro de la aplicación; si estos datos son manipulados por un atacante**, pueden desencadenar la ejecución de código arbitrario en el sistema afectado**. Esto podría permitir comprometer completamente el servidor SAP, manipular información empresarial o facilitar movimientos laterales hacia otros sistemas dentro de la red corporativa.

Por otro lado, la vulnerabilidad CVE-2026-27689, con una puntuación **CVSS de 7.7 (alta),** afecta a SAP Supply Chain Management y se debe a un problema de consumo excesivo de recursos dentro de un módulo de función habilitado remotamente. Un atacante autenticado puede explotar esta debilidad invocando repetidamente una función con parámetros manipulados que provocan la **ejecución de bucles prolongados dentro del sistema**. Esto genera un consumo elevado de CPU y memoria, lo que puede derivar en condiciones de Denial-of-Service (DoS) que afecten la disponibilidad de servicios críticos relacionados con la gestión de la cadena de suministro.

Solución y mitigaciones:

SAP ha publicado parches oficiales para corregir ambas vulnerabilidades a través de sus **Security Notes** incluidas en el ciclo de actualizaciones de marzo de 2026, mismas que puedes encontrar en los siguientes enlaces:

https://me.sap.com/notes/3714585

https://me.sap.com/notes/3719502

Para **CVE-2026-27685**, la **SAP Security Note 3714585** introduce validaciones adicionales para impedir que datos serializados maliciosos sean procesados por el sistema. En el caso de **CVE-2026-27689**, la **SAP Security Note 3719502** corrige el manejo de parámetros dentro del módulo de función afectado y limita la ejecución de bucles que podrían provocar agotamiento de recursos.

Además de aplicar los parches oficiales, SAP recomienda a las organizaciones implementar controles adicionales de seguridad, tales como:

- restringir las capacidades de carga de contenido únicamente a usuarios confiables
- revisar periódicamente los registros de actividad en busca de comportamientos anómalos
- limitar el acceso a módulos de función remotos
- monitorear el uso de recursos del sistema para detectar posibles intentos de explotación.

Información adicional:

- https://onapsis.com/blog/sap-security-patch-day-march-2026/
- https://nvd.nist.gov/vuln/detail/CVE-2026-27689
- https://nvd.nist.gov/vuln/detail/CVE-2026-27685
- Vulnerabilidades en productos SAP – CERT-PY