SAP parcheó una vulnerabilidad crítica que afecta el componente del Asistente de Configuración de LM en la plataforma Java de NetWeaver Application Server (AS), que permitía a un atacante no autenticado tome el control de las aplicaciones SAP.

El error, denominado RECON y rastreado como CVE-2020-6287, está calificado con una puntuación CVSS máxima de 10, lo que podría afectar a más de 40 mil clientes de SAP, según la compañía de seguridad cibernética Onapsis.

> *«Si se explota con éxito, un atacante remoto no autenticado puede obtener acceso sin restricciones a los sistemas SAP mediante la creación de usuarios con altos privilegios y la ejecución de comandos arbitrarios del sistema operativo con los privilegios de la cuenta de usuario del servicio SAP, que tiene acceso sin restricciones a la base de datos SAP y puede realizar actividades de mantenimiento de aplicaciones, como cerrar aplicaciones federadas SAP»*, dijo la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA).
>
> *«La confidencialidad, integridad y disponibilidad de los datos y procesos alojados por la aplicación SAP están en riesgo por esta vulnerabilidad»,* agregó.

La vulnerabilidad está presente de forma predeterminada en las aplicaciones de SAP que se ejecutan sobre SAP NerWeaver AS Java 7.3 y posteriores (hasta SAP NetWeaver 7.5), lo que pone en riesgo muchas soluciones empresariales de SAP, incluidas SAP Enterprise Resource Planning, SAP Product Lifecycle Management, SAP Customer Relationship Management, SAP Supply Chain Management, SAP Business Intelligence y SAP Enterprise Portal.

Según Onapsis, RECON se debe a una falta de autenticación en el componente web de SAP NetWeaver AS para Java, lo que le permite a un atacante realizar actividades con privilegios elevados en el sistema SAP susceptible.

> *«Un atacante remoto no autenticado puede explotar esta vulnerabilidad a través de una interfaz HTTP, que generalmente está expuesta a los usuarios finales y, en muchos casos, a Internet»,* dijo CISA.

Al explotar la falla para crear un nuevo usuario de SAP con privilegios máximos, el intruso puede comprometer las instalaciones de SAP para ejecutar comandos arbitrarios, como modificar o extraer información altamente sensible, así como interrumpir procesos críticos del negocio.

Aunque no existe evidencia de una explotación activa de la vulnerabilidad, CISA advirtió que la disponibilidad de los parches podría facilitar a los adversarios realizar ingeniería inversa de la falla para crear exploits y atacar sistemas sin parches.