Alerta de seguridad cibernética	9VSA20-00271-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de julio de 2020
Última revisión	16 de julio de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por el Equipo de respuesta de seguridad de productos de SAP, referente a una vulnerabilidad crítica que afecta al asistente de configuración LM del componente Java del servidor de aplicaciones SAP NetWeaver (AS). El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-6287

Impacto

La vulnerabilidad crítica afecta a su componente NetWeaver AS para Java. Esta vulnerabilidad puede comprometer las instalaciones vulnerables de SAP, incluida la modificación o extracción de información altamente confidencial, así como la interrupción de los procesos comerciales críticos. 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. Al tomar el Protocolo de transferencia de hipertexto (HTTP), el atacante podría tomar el control de aplicaciones SAP confiables y crear usuarios con privilegios elevados y ejecutar comandos arbitrarios del sistema operativo con los privilegios de la cuenta de usuario del servicio SAP (<sid>adm), que tiene acceso sin restricciones a la base de datos de SAP y puede realizar actividades de mantenimiento de aplicaciones, como cerrar aplicaciones de SAP federadas. La confidencialidad, integridad y disponibilidad de los datos y procesos alojados por la aplicación SAP están en riesgo por esta vulnerabilidad.

La vulnerabilidad se introduce debido a la falta de autenticación en un componente web de SAP NetWeaver AS para Java que permite varias actividades de alto privilegio en el sistema SAP.

Productos afectados

Esta vulnerabilidad está presente de forma predeterminada en las aplicaciones de SAP que se ejecutan sobre SAP NetWeaver AS Java 7.3 y cualquier versión más reciente (hasta SAP NetWeaver 7.5). Las soluciones empresariales de SAP potencialmente vulnerables incluyen cualquier solución basada en Java de SAP como (pero no limitado a):

- SAP Enterprise Resource Planning,
- SAP Product Lifecycle Management,
- SAP Customer Relationship Management,
- SAP Supply Chain Management,
- Gestión de relaciones con proveedores de SAP,
- SAP NetWeaver Business Warehouse,
- SAP Business Intelligence,
- Infraestructura móvil SAP NetWeaver,
- SAP Enterprise Portal,
- SAP Process Orchestration / Process Integration),
- SAP Solution Manager,
- Infraestructura de desarrollo de SAP NetWeaver,
- SAP Central Process Scheduling,
- SAP NetWeaver Composition Environment, y
- SAP Landscape Manager.

Mitigación y Enlaces

Mitigación

Se recomienda aplicar las actualizaciones publicadas por el fabricante a partir de la nota de seguridad de SAP #2934135, por sobre mitigaciones individuales.

Enlaces

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6287
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675
https://www.onapsis.com/recon-sap-cyber-security-vulnerability
https://www.sap.com/australia/about/trust-center/security.html
https://wiki.scn.sap.com/wiki/display/PSR/The+Official+SAP+Product+Security+Response+Space