Los hackers han estado fijando activamente sus objetivos en aplicaciones SAP no seguras como un intento por robar información y sabotear procesos críticos, según una nueva investigación.

> *«La explotación observada podría conducir en muchos casos a un control total de la aplicación SAP no segura, evitando los controles comunes de seguridad y cumplimiento, y permitiendo a los atacantes robar información confidencial, realizar fraudes financieros o interrumpir los procesos comerciales de misión crítica mediante la implementación de ransomware o la detención de operaciones»,* dijeron la compañía de seguridad Onapsis y SAP en un informe conjunto.

La compañía con sede en Boston, dijo que detectó más de 300 explotaciones exitosas de un total de 1500 intentos dirigidos a vulnerabilidades previamente conocidas y configuraciones inseguras específicas para sistemas SAP entre mediados de 2020 y marzo de 2021, con múltiples intentos de fuerza bruta realizados por adversarios dirigidos a privilegiar las cuentas de SAP y encadenar varias vulnerabilidades para atacar las aplicaciones de SAP.

Las aplicaciones que se han dirigido incluyen, entre otras, la planificación de recursos empresariales (ERP), la gestión de cadena de suministro (SCM), la gestión del capital humano (HCM), la gestión del ciclo de vida del producto (PLM), la gestión de relaciones con el cliente (CRM), entre otras.

Algo que causa preocupación es que el informe de Onapsis describe el armamentismo de las vulnerabilidades de SAP en menos de 72 horas desde el lanzamiento de los parches, con nuevas aplicaciones de SAP no protegidas aprovisionadas en entornos de nube que se descubren y ponen en peligro en menos de 3 horas.

En un caso, un día después de que SAP emitiera un parche para CVE-2020-6287 el 14 de julio de 2020, surgió un exploit de prueba de concepto en la naturaleza, que fue seguido por una actividad de escaneo masivo el 16 de julio y el lanzamiento de un exploit público completamente funcional el 17 de junio de 2020.

Los vectores de ataque no estuvieron faltos de sofisticación. Se encontró que los atacantes adoptaron un conjunto variado de técnicas, herramientas y procedimientos para obtener acceso inicial, escalar privilegios, eliminar shells web para la ejecución de comandos arbitrarios, crear usuario administradores de SAP con altos privilegios e incluso extraer credenciales de base de datos. Los propios ataques se lanzaron con la ayuda de nodos TOR y servidores privados virtuales distribuidos (VPS).

Las seis vulnerabilidades explotadas por los actores de amenazas son:

- CVE-2010-5326 (puntuación CVSS: 10) – Defecto de ejecución de código remoto en SAP NetWeaver Application Server (AS) de Java.
- CVE-2016-3976 (puntuación CVSS: 7.5) – Vulnerabilidad de recorrido de directorio en SAP NetWeaver AS Java.
- CVE-2016-9563 (puntuación CVSS: 6.4) – Vulnerabilidad de expansión de entidad externa XML (XXE) en el componente BC-BMT-BPM-DSK de SAP NetWeaver AS Java.
- CVE-2018-2380 (puntuación CVSS: 6.6) – Vulnerabilidad transversal de directorio en el componente de ventas por Internet en SAP CRM.
- CVE-2020-6207 (puntuación CVSS: 9.8) – Comprobación de autenticación faltante en SAP Solution Manager.
- CVE-2020-6287 (puntuación CVSS: 10) – Fallo de RECON (también conocido como código explotable de forma remota en NetWeaver) en el componente del asistente de configuración de LM.

Revelado por primera vez en julio de 2020, la explotación exitosa de CVE-2020-6287, podría otorgar a un atacante no autenticado acceso completo al sistema SAP afectado, contando la *«capacidad de modificar registros financieros, robar información de identificación personal (PII) de empleados, clientes y proveedores, corromper los datos, eliminar o modificar registros y rastreos y otras acciones que ponen en riesgo las operaciones comerciales esenciales, la ciberseguridad y el cumplimiento normativo».*

Onapsis también dijo que pudo detectar actividad de escaneo para CVE-2020-6207, que se remonta al 19 de octubre de 2020, casi tres meses antes del lanzamiento público de un exploit en pleno funcionamiento el 14 de enero de 2021, lo que implica que los actores de amenazas tenían conocimiento del exploit antes de la divulgación pública.

Además, se descubrió que un ataque separado observado el 9 de diciembre, encadenaba exploits para tres vulnerabilidades, CVE-2020-6287 para crear un usuario administrador e iniciar sesión en el sistema SAP, CVE-2018-2380 para escalar privilegios y CVE-2016-3976 para acceder a cuentas con privilegios elevados y a la base de datos.

«Todo esto sucedió en 90 minutos», dijeron los investigadores de Onapsis.

Aunque no se han descubierto infracciones de clientes, tanto SAP como Onapsis instan a las empresas a realizar una evaluación de compromiso de las aplicaciones, aplicar los parches relevantes y abordar las configuraciones incorrectas para evitar el acceso no autorizado.

> *«Los hallazgos críticos describen ataques a vulnerabilidades con parches y pautas de configuración segura disponibles durante meses e incluso años. Desafortunadamente, demasiadas organizaciones todavía operan con una brecha de gobernanza importante en términos de seguridad cibernética y cumplimiento de sus aplicaciones de misión crítica, lo que permite que los actores de amenazas externos e internos accedan, se infiltren y obtengan el control total de su información y procesos más sensibles y regulado»,* dijo Mariano Nunez, CEO de Onapsis.

> *«Las empresas que no han priorizado la mitigación rápida de estos riesgos conocidos deben considerar que sus sistemas están comprometidos y tomar medidas inmediatas y apropiadas»,* agregó.