BOLETÍN DE ALERTA

Boletín Nro.: 2024-12
Fecha de publicación: 17/05/2024
Tema: Vulnerabilidades críticas en productos SAP

Productos afectados:
-SAP Commerce, versión -HY_COM 2205
-SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758.

Descripción:

Se han reportado vulnerabilidades críticas que afectan a soluciones SAP, las cuales se describen a continuación:

Vulnerabilidad en SAP CX Commerce identificada como CVE-2019-17495 con una puntuación CVSSv3 de 9.8, una vulnerabilidad de inyección de Cascading Style Sheets (CSS) en Swagger UI podría permitir a un actor malicioso realizar Overwrite de Ruta Relativa (RPO) para realizar la exfiltración de valor de campo de entrada basada en CSS, como la exfiltración del valor de un token CSRF.

Vulnerabilidad de subida de archivo en SAP NetWeaver Application Server ABAP y ABAP Platform identificada como CVE-2024-33006 con una puntuación CVSSv3 de 9.6, una vulnerabilidad que podría permitir a un actor malicioso no autenticado subir un archivo malicioso en el servidor, que cuando es accedido por la víctima puede comprometer el sistema.

Impacto:

Estas vulnerabilidades podrían permitir a un actor malicioso la inserción de datos JSON no confiables desde servidores remotos y comprometer el sistema a través de la subida de un archivo malicioso.

Recomendación:

Se recomienda realizar las actualizaciones de los productos afectados desde la página oficial del fabricante.

Para verificar el listado completo de vulnerabilidades, ingresar al siguiente enlace:
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2024.html

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-mayo-de-2024
- https://www.cve.org/CVERecord?id=CVE-2024-33006
- https://www.cve.org/CVERecord?id=CVE-2024-28165
- https://www.cve.org/CVERecord?id=CVE-2024-32730