BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-22
Fecha de publicación: 14/08/2024
Tema: Vulnerabilidad crítica de autenticación en la plataforma SAP
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- BusinessObjects Business Intelligence versions 430 y 440

Descripción

SAP ha lanzado su paquete de parches de seguridad para agosto de 2024, abordando 17 vulnerabilidades, incluida una omisión de autenticación crítica que podría permitir a atacantes remotos comprometer por completo el sistema.

Entre las vulnerabilidades más relevantes se destaca la identificada como CVE-2024-41730, calificada con una puntuación de 9.8 en el sistema CVSS v3.1. Este fallo de "verificación de autenticación faltante" afecta a las versiones 430 y 440 de SAP BusinessObjects Business Intelligence Platform y es explotable bajo ciertas condiciones.

En SAP BusinessObjects Business Intelligence Platform, si el inicio de sesión único (SSO) está habilitado en la autenticación empresarial, un usuario no autorizado podría obtener un token de inicio de sesión a través de un punto de conexión REST. Esto permitiría al atacante comprometer completamente el sistema, afectando gravemente la confidencialidad, integridad y disponibilidad de los datos y servicios de inteligencia empresarial.

Actualmente, esta vulnerabilidad está en proceso de análisis y aún no se dispone de toda la información

Aquí se destacan algunas de las vulnerabilidades más relevantes corregidas:

- CVE-2024-42374: Inyección XML en el servicio web de exportación de SAP BEx Web Java Runtime
  El servicio web de exportación de BEx Web Java Runtime no valida adecuadamente un documento XML recibido de una fuente no confiable. Un atacante podría recuperar información del sistema SAP ADS y agotar el servicio XMLForm, lo que provocaría la indisponibilidad de la funcionalidad de creación de PDF en SAP ADS. Esto compromete la confidencialidad y la disponibilidad de la aplicación.

- **CVE-2024-29415:** Vulnerabilidad de Server-Side Request Forgery (SSRF) en aplicaciones desarrolladas con SAP Build Apps
  El paquete `ip`, hasta la versión 2.0.1 para Node.js, podría permitir ataques SSRF, ya que ciertas direcciones IP (como 127.1, 01200034567, 012.1.2.3, 000:0:0000::01 y ::fFFf:127.0.0.1) están clasificadas incorrectamente como enrutables globalmente a través de `isPublic`. Cabe señalar que este problema persiste debido a una corrección incompleta para la vulnerabilidad CVE-2023-42282.

Solución

Hay parches disponibles para las siguientes versiones:

- SERVIDORES DE LA PLATAFORMA SBOP BI 4.3 – Nivel de parche SP005
- SERVIDORES DE LA PLATAFORMA SBOP BI 2025 – Nivel de parche SP00
- SERVIDORES DE LA PLATAFORMA SBOP BI 4.3 – Nivel de parche SP004

Información adicional:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html
- https://redrays.io/blog/critical-sap-businessobjects-authentication-vulnerability-cve-2024-41730/
- https://www.csa.gov.sg/alerts-advisories/security-bulletins/sb-2024-033
- https://nvd.nist.gov/vuln/detail/CVE-2024-41730
- https://accounts.sap.com/saml2/idp/sso
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html?anchorId=section_370125364

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com