Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00804-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de marzo de 2023
Última revisión	17 de marzo de 2023

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

<u>Resumen</u>

El CSIRT de Gobierno comparte información de las vulnerabilidades entregadas por SAP para sus productos Business Objects, NetWeaver, ERP y S4HANA.

Vulnerabilidades

CVE-2023-25616	
CVE-2023-25617	CVE-2023-27270
CVE-2023-23857	CVE-2023-27271
CVE-2023-27269	CVE-2023-27896
CVE-2023-27500	CVE-2023-27894
CVE-2023-27893	CVE-2023-26457
CVE-2023-27501	CVE-2023-27895
CVE-2023-26459	CVE-2023-0021
CVE-2023-27498	CVE-2023-27268
CVE-2023-26461	CVE-2023-26460
CVE-2023-25615	

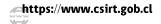
Impacto

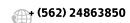
Vulnerabilidades de riesgo crítico

CVE-2023-25616: Error de inyección de código en la Central Management Console (CMC). Afecta a SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430.

CVE-2023-23857: Error de control inapropiado de acceso en SAP NetWeaver AS para Java.

CVE-2023-27269: Vulnerabilidad Directory Traversal en SAP NetWeaver AS para ABAP y ABAP Platform. CVE-2023-27500: Vulnerabilidad Directory Traversal en SAP NetWeaver AS para ABAP y ABAP Platform (SAPRSBRO Program).







Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



CVE-2023-25617: Vulnerabilidad de ejecución de comandos OS en SAP Business Objects Business Intelligence Platform (Adaptive Job Server).

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430

SAP NetWeaver AS for Java, versión 7.50.

SAP NetWeaver Application Server para ABAP y ABAP Platform, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.

SAP NetWeaver Application Server para ABAP y ABAP Platform (SAPRSBRO Program), versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.

SAP Business Objects (Adaptive Job Server), versiones 420, 430.

Enlaces

https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25616

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25617

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23857

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27269

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27500

