Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00547-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2022
Última revisión	13 de enero de 2022

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 del Gobierno de Chile, CSIRT de Gobierno, comparte nuevas vulnerabilidades en productos de SAP.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-44228
CVE-2022-22531
CVE-2021-44235
CVE-2021-42066
CVE-2021-44234
CVE-2022-22529
CVE-2022-42067
CVE-2021-42068
CVE-2021-42070
CVE-2021-42069
CVE-2021-44233

Impactos

Vulnerabilidades de riesgo alto:

CVE-2021-44228: Ejecución Remota de Código relacionada con el componente Apache Log4j2.

CVE-2022-22531: Vulnerabilidad en la aplicación Create Single Payment de SAP S/4HANA.

CVE-2021-44235: Vulnerabilidad de inyección de código en utility class en SAP NetWeaver AS ABAP.

Productos afectados

CVE-2021-44228: SAP Customer Checkout.
SAP BTP Cloud Foundry.

SAP Landscape Management.
SAP Connected Health Platform 2.0 – Fhirserver.
SAP HANA XS Advanced Cockpit.
SAP NetWeaver Process Integration (Java Web Service Adapter).
SAP HANA XS Advanced.
Internet of Things Edge Platform.
SAP BTP Kyma.
SAP Enable Now Manager.
SAP Cloud for Customer (add-in for Lotus notes client).
SAP Localization Hub, digital compliance service for India.
SAP Edge Services On Premise Edition.
SAP Edge Services Cloud Edition.
SAP BTP API Management (Tenant Cloning Tool).
SAP NetWeaver ABAP Server and ABAP Platform (Adobe LiveCycle Designer 11.0).
SAP Digital Manufacturing Cloud for Edge Computing.
SAP Enterprise Continuous Testing by Tricentis.
SAP Cloud-to-Cloud Interoperability.
Reference Template for enabling ingestion and persistence of time series data in Azure.
SAP Business One.

CVE-2022-22531: SAP S/4HANA, Versiones 100, 101, 102, 103, 104, 105, 106.

CVE-2021-44235: SAP NetWeaver AS ABAP, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=596902035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44235
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42066
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44234
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22529
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42067
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42068
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42070
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42069
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44233

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.13 15:35:34 -03'00'