Alerta de seguridad cibernética	9VSA21-00422-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de abril de 2021
Última revisión	13 de abril de 2021

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, CSIRT, comparte información sobre sobre nuevas vulnerabilidades y actualizaciones comunicadas por SAP durante su Security Patch Day de abril 2021.

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

Vulnerabilidades

CVE-2021-27602
CVE-2021-21482
CVE-2021-21483
CVE-2021-27608
CVE-2021-21485
CVE-2021-27598
CVE-2021-27603
CVE-2021-27599
CVE-2021-27604
CVE-2021-27600
CVE-2021-27601
CVE-2021-27609
CVE-2021-21492
CVE-2021-27605
Actualización relacionada con CVE-2021-21481
Actualización relacionada con CVE-2020-26832
Actualización relacionada con CVE-2021-21491

Impactos

Las vulnerabilidades descritas como de riesgo crítico son las siguientes.

CVE-2021-27602 Ejecución remota de código en SAP Commerce.
Actualización relacionada con CVE-2021-21481 Falta de validación de autorización en SAP NetWeaver AS Java (MigrationService).
Actualización a la Security Note de Agosto de 2018 para Google Chromium con SAP Business Client 6.5.

De riesgo alto:

CVE-2021-21482 Revelación de información en SAP NetWeaver Master Data Management.
CVE-2021-21483 Revelación de información en SAP Solution Manager.
CVE-2021-21485 Revelación de información en SAP NetWeaver AS para Java.
Actualización relacionada con CVE-2020-26832 Falta de validación de autorización en SAP NetWeaver AS ABAP y SAP S4 HANA.

Productos Afectados

Google Chromium con SAP Business Client 6.5.
SAP Commerce, versiones de la 1808 a la 2011.
SAP NetWeaver Master Data Management, versions 710 y 710.750.
SAP Solution Manager 7.20.
SAP NetWeaver AS para Java.
SAP NetWeaver AS para ABAP, versions 731, 740 y 750.
SAP NetWeaver AS ABAP y SAP S4 HANA.
SAP Setup 9.0.
SAP Process Integration (Integration Builder Framework), versiones 7.10 a la 7.50.
SAP Manufacturing Execution (System Rules) versions 15.1 a 15.4.
SAP Focused RUN versions 200, 300.
SAP Fiori Apps 2.0 for Travel Management en SAP ERP, version 608.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27602
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21482
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21483
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27608
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21485
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27598
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27603
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27599

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27604
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27600
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27601
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27609
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21481
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21491

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.13 22:24:11 -04'00'