Alerta de seguridad cibernética	9VSA21-00464-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2021
Última revisión	7 de julio 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades que afectan a la plataforma ERP Sage X3.

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

Vulnerabilidades

CVE-2020-7387
CVE-2020-7388
CVE-2020-7389
CVE-2020-7390

Impactos

Como crítica es considerada la vulnerabilidad CVE-2020-7388, que permite la ejecución de comandos remotos con elevados privilegios en el componente AdxDSrv.exe. Las demás vulnerabilidades son consideradas como de severidad media.

Productos Afectados

Sage X3 9, X3 HR & Payroll Version 9, X3 11, y X3 12.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://www.rapid7.com/blog/post/2021/07/07/cve-2020-7387-7390-multiple-sage-x3-vulnerabilities/
https://www.sagecity.com/gb/sage-x3-uk/f/sage-x3-uk-announcements-news-and-alerts/148233/sage-x3-version-11-june-2021
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2020-7387
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2020-7388
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2020-7389
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2020-7390

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.07 16:19:32 -04'00'