Alerta de seguridad cibernética	9VSA23-00780-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de febrero de 2023
Última revisión	2 de febrero 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.

Resumen

El CSIRT de Gobierno comparte información sobre tres vulnerabilidades que afecta a OpenEMR, sistema usado por organizaciones de salud. Dos de las vulnerabilidades permiten, de ser explotadas de forma combinadas, la ejecución remota de código (RCE).

Las vulnerabilidades son resueltas en OpenEMR versión 7.0.0.

Vulnerabilidades

CVE no disponible
CVE no disponible
CVE no disponible

Impacto

Vulnerabilidades de riesgo crítico

Dos de las vulnerabilidades pueden ser usadas de forma combinada para ejecutar comandos arbitrarios de sistema en cualquier servidor OpenEMR, y así robar datos sensibles de los pacientes, pudiendo en el peor de los casos comprometer a toda la infraestructura crítica.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

OpenEMR anteriores a la versión 7.0.0.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.02 12:44:20 -03'00'

Enlaces

https://www.sonarsource.com/blog/openemr-remote-code-execution-in-your-healthcare-system/
https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#7.0.0_Patch_.2811.2F30.2F22.29

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob