Alerta de seguridad cibernética	9VSA23-00850-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	16 de junio de 2023
Última revisión	16 de junio 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 de vulnerabilidades críticas en MOVEit Transfer, programa para la administración de la transferencia de archivos. Progress, proveedora de MOVEit, ya ha publicado los respectivos parches.

Vulnerabilidades

CVE-2023-34362
CVE-2023-35036

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-34362: Vulnerabilidad de inyección SQL que permite elevación de privilegios y acceso no autorizado. Para evitar su explotación, los desarrolladores llaman a bloquear el tráfico externo a los puertos 80 y 443, entendiendo que esto impedirá algunas de las funciones de MOVEit Automation y plugins. Los desarrolladores también llaman a revisar la carpeta 'c[:]\MOVEit Transfer\wwwroot\' en busca de archivos sospechosos o respaldos inesperados.

El grupo de ransomware Cl0p ha señalado haber usado esta vunerabilidad para robar datos en múltiples ataques.

CVE-2023-35036: Vulnerabilidad de inyección SQL que permite a atacantes robar información de las bases de datos de los usuarios.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

MOVEit Transfer 2023.0.0
MOVEit Transfer 2022.1.x
MOVEit Transfer 2022.0.x
MOVEit Transfer 2021.1.x
MOVEit Transfer 2021.0.x

Enlaces

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34362
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35036

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.16 11:23:57 -04'00'