Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00707-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre 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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre una vulnerabilidad en Zoho ManageEngine.

Vulnerabilidad

CVE-2022-35405

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-35405: Vulnerabilidad de ejecución remota de código.
La agencia federal encargada de la ciberseguridad en EE.UU. (CISA) agregó esta vulnerabilidad recientemente a su lista de vulnerabilidades conocidamente explotadas.

Productos afectados

Access Manager Plus versión 4302 y anteriores.
Password Manager Pro versión 12100 y anteriores.
PAM360 versión 5500 y anteriores.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.26 15:50:38 -03'00'

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.cisa.gov/uscert/ncas/current-activity/2022/09/23/cisa-has-added-one-known-exploited-vulnerability-catalog
https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-35405.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35405