Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00502-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de octubre de 2021
Última revisión	06 de octubre 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 relacionada con una vulnerabilidad de riesgo alto que afecta a Apache HTTP Server 2.4.49.

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

Vulnerabilidad

CVE-2021-41773

Impactos

Una falla encontrada en Apache HTTP Server 2.4.49 permite a un atacante usar un ataque de salto de directorio (path traversal) para mapear archivos URL fuera del root de documentos esperado.

Productos Afectados

Apache HTTP Server 2.4.49.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://httpd.apache.org/security/vulnerabilities_24.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.06 12:27:11 -03'00'