

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00920-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	16 de octubre de 2023
Última revisión	16 de octubre 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 recientes actualizaciones críticas de seguridad publicadas por Progress para su programa WS_FTP Server.

Vulnerabilidades

CVE-2023-42657
CVE-2023-40045
CVE-2023-40047
CVE-2023-40046
CVE-2023-40048
CVE-2022-27665
CVE-2023-40049

Impacto

Vulnerabilidad crítica

CVE-2023-40044: Un atacante pre-autenticado podría aprovechar esta vulnerabilidad de deserialización .NET en el módulo Ad Hoc Transfer para ejecutar comandos remotos en el sistema operativo WS_FTP subyacente. CVSS: 10.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

WS_FTP Server versiones anteriores a 8.7.4 y 8.8.2.

Enlaces

<https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42657>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40045>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40047>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40046>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40048>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27665>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40049>