Alerta de seguridad cibernética	9VSA21-00488-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de septiembre de 2021
Última revisión	08 de septiembre 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 sobre una nueva vulnerabilidad zero-day crítica anunciada por Microsoft y que afecta a su producto Microsoft Windows.

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

Vulnerabilidades

CVE-2021-40444

Impactos

Esta vulnerabilidad corresponde a un error que permite la ejecución remota de código y que afecta a MSHTML (también conocido como Trident), motor del navegador Internet Explorer pero que también es usado por los programas de Office. La vulnerabilidad puede ser explotada a través de documentos de Office especialmente diseñados para tal efecto.

Productos Afectados

Microsoft Windows

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor cuando estas estén disponibles. Mientras tanto, usar la vista protegida o Application Guard for Office al abrir documentos descargados de internet y desactivar los controles ActiveX en Internet Explorer hasta que se haya instalado un parche.

Enlaces

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/11231-ccn-cert-av-21-21-vulnerabilidad-critica-que-afecta-a-microsoft-office.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444