

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	9VSA23-00897-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	12 de septiembre de 2023
Última revisión	12 de septiembre 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 afectada a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de las vulnerabilidades parchadas por Microsoft como parte de su actualización mensual Update Tuesday, correspondiente a septiembre de 2023.

Vulnerabilidades

CVE-2023-4863	CVE-2023-38144	CVE-2023-36793	CVE-2023-36759
CVE-2023-41764	CVE-2023-38143	CVE-2023-36792	CVE-2023-36758
CVE-2023-39956	CVE-2023-38142	CVE-2023-36788	CVE-2023-36757
CVE-2023-38164	CVE-2023-38141	CVE-2023-36777	CVE-2023-36756
CVE-2023-38163	CVE-2023-38140	CVE-2023-36773	CVE-2023-36745
CVE-2023-38162	CVE-2023-38139	CVE-2023-36772	CVE-2023-36744
CVE-2023-38161	CVE-2023-36886	CVE-2023-36771	CVE-2023-36742
CVE-2023-38160	CVE-2023-36805	CVE-2023-36770	CVE-2023-36740
CVE-2023-38156	CVE-2023-36804	CVE-2023-36767	CVE-2023-36739
CVE-2023-38155	CVE-2023-36803	CVE-2023-36766	CVE-2023-36736
CVE-2023-38152	CVE-2023-36802	CVE-2023-36765	CVE-2023-35355
CVE-2023-38150	CVE-2023-36801	CVE-2023-36764	CVE-2023-33136
CVE-2023-38149	CVE-2023-36800	CVE-2023-36763	CVE-2023-32051
CVE-2023-38148	CVE-2023-36799	CVE-2023-36762	CVE-2023-29332
CVE-2023-38147	CVE-2023-36796	CVE-2023-36761	CVE-2023-24936
CVE-2023-38146	CVE-2023-36794	CVE-2023-36760	CVE-2022-41303

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-38148: Vulnerabilidad de ejecución remota de código en Internet Connection Sharing (ICS).
CVSS: 7.7.

CVE-2023-36796: Vulnerabilidad de ejecución remota de código en Visual Studio. CVSS: 7.8

CVE-2023-36793: Vulnerabilidad de ejecución remota de código en Visual Studio. CVSS: 7.8

CVE-2023-36792: Vulnerabilidad de ejecución remota de código en Visual Studio. CVSS: 7.8.
CVE-2023-29332: Vulnerabilidad de elevación de privilegios en Microsoft Azure Kubernetes Service.
CVSS: 7.5.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

.NET and Visual Studio	Microsoft Office Word
.NET Core & Visual Studio	Microsoft Streaming Service
.NET Framework	Microsoft Windows Codecs Library
3D Builder	Servicing Stack Updates
3D Viewer	Visual Studio
Azure DevOps	Visual Studio Code
Azure HDInsights	Windows Cloud Files Mini Filter Driver
Microsoft Azure Kubernetes Service	Windows Common Log File System Driver
Microsoft Dynamics	Windows Defender
Microsoft Dynamics Finance & Operations	Windows DHCP Server
Microsoft Edge (Chromium-based)	Windows GDI
Microsoft Exchange Server	Windows Internet Connection Sharing (ICS)
Microsoft Identity Linux Broker	Windows Kernel
Microsoft Office	Windows Scripting
Microsoft Office Excel	Windows TCP/IP
Microsoft Office Outlook	Windows Themes
Microsoft Office SharePoint	

Enlaces

<https://msrc.microsoft.com/update-guide/releaseNote/2023-Sep>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4863>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41764>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39956>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38164>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38163>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38162>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38161>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38160>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38156>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38155>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38152>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38150>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38149>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38148>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38147>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38146>

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-2023-38144>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38143>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38142>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38141>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38140>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38139>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36886>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36805>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36804>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36803>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36802>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36801>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36800>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36799>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36796>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36794>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36793>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36792>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36788>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36777>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36773>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36772>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36771>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36770>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36767>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36766>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36765>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36764>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36763>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36762>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36761>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36760>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36759>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36758>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36757>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36756>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36745>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36744>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36742>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36740>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36739>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36736>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35355>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33136>

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-2023-32051>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29332>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24936>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41303>