| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00702-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de septiembre de 2022 |
| Última revisión | 13 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 nuevas vulnerabilidades comunicadas por Microsoft en su Update Tuesday correspondiente a septiembre 2022.

## Vulnerabilidades

CVE-2022-26929
CVE-2022-38013
CVE-2022-38009
CVE-2022-38008
CVE-2022-38007
CVE-2022-35803
CVE-2022-38011
CVE-2022-37959
CVE-2022-38006
CVE-2022-37958
CVE-2022-37964
CVE-2022-37963
CVE-2022-37962
CVE-2022-38010
CVE-2022-37961
CVE-2022-38005
CVE-2022-37957
CVE-2022-38004
CVE-2022-37956
CVE-2022-37955
CVE-2022-37954
CVE-2022-34734
CVE-2022-34733
CVE-2022-34732
CVE-2022-34731
CVE-2022-34730
CVE-2022-34729
CVE-2022-34728
CVE-2022-34727
CVE-2022-34726
CVE-2022-34725
CVE-2022-34724
CVE-2022-34723
CVE-2022-34722
CVE-2022-34721
CVE-2022-34720
CVE-2022-34718
CVE-2022-34719
CVE-2022-35841
CVE-2022-35840
CVE-2022-35838
CVE-2022-35837
CVE-2022-35836
CVE-2022-35835
CVE-2022-35834
CVE-2022-35833
CVE-2022-35832
CVE-2022-35831
CVE-2022-35830
CVE-2022-35828
CVE-2022-35823
CVE-2022-33679
CVE-2022-33647
CVE-2022-30200
CVE-2022-30196
CVE-2022-30170
CVE-2022-26928
CVE-2022-23960
CVE-2022-34700
CVE-2022-35805

CVE-2022-38020 CVE-2022-38019 CVE-2022-37969

# Impacto

### Vulnerabilidades de riesgo crítico

CVE-2022-34722: Ejecución remota de código en Windows Internet Key Exchange (IKE) Protocol Extensions
CVE-2022-34721: Ejecución remota de código en Windows Internet Key Exchange (IKE) Protocol Extensions.
CVE-2022-34718: Ejecución remota de código en Windows TCP/IP
CVE-2022-34700: Ejecución remota de código en Microsoft Dynamics CRM (on-premises).
CVE-2022-35805: Ejecución remota de código en Microsoft Dynamics CRM (on-premises).

### Productos afectados

AV1 Video Extension
Azure ARC
Microsoft .NET Framework 3.5 AND 4.8
Microsoft Defender for Endpoint for Mac
Microsoft Dynamics CRM (on-premises) 9.1
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server Subscription Edition
Microsoft Visio 2016 (64-bit edition)
Microsoft Visual Studio 2022 version 17.2
Raw Image Extension
Visual Studio Code
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows RT 8.1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016 (Server Core installation)

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces

https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26929
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35803

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37957
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34734
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34732
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34730
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34728
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34727
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34726
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34725
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34725
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34722
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34721
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34718
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34719
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35837
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35836
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35833
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33679

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30200
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30196
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30170
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26928
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37969

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.13 17:36:43 -03'00'