

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	9VSA23-00914-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	10 de octubre de 2023
Última revisión	10 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 la actualización mensual de seguridad de Microsoft, conocida como Update Tuesday, correspondiente a octubre de 2023.

Vulnerabilidades

CVE-2023-36602	CVE-2023-36420	CVE-2023-36790	CVE-2023-36592
CVE-2023-36720	CVE-2023-36568	CVE-2023-38166	CVE-2023-36593
CVE-2023-36724	CVE-2023-36721	CVE-2023-36435	CVE-2023-36594
CVE-2023-36725	CVE-2023-36417	CVE-2023-36902	CVE-2023-36596
CVE-2023-36431	CVE-2023-38171	CVE-2023-35349	CVE-2023-36603
CVE-2023-36434	CVE-2023-36418	CVE-2023-36785	CVE-2023-36605
CVE-2023-36433	CVE-2023-36419	CVE-2023-36564	CVE-2023-36606
CVE-2023-36557	CVE-2023-36730	CVE-2023-36565	CVE-2023-36697
CVE-2023-36778	CVE-2023-36429	CVE-2023-36567	CVE-2023-36698
CVE-2023-36436	CVE-2023-36717	CVE-2023-36571	CVE-2023-36701
CVE-2023-36576	CVE-2023-36718	CVE-2023-36572	CVE-2023-36702
CVE-2023-36598	CVE-2023-36726	CVE-2023-36573	CVE-2023-36703
CVE-2023-36438	CVE-2023-36737	CVE-2023-36574	CVE-2023-36704
CVE-2023-36563	CVE-2023-36415	CVE-2023-36575	CVE-2023-36706
CVE-2023-36722	CVE-2023-36416	CVE-2023-36577	CVE-2023-36707
CVE-2023-36569	CVE-2023-36723	CVE-2023-36578	CVE-2023-36709
CVE-2023-36570	CVE-2023-36728	CVE-2023-36579	CVE-2023-36710
CVE-2023-36731	CVE-2023-41773	CVE-2023-36581	CVE-2023-36711
CVE-2023-36732	CVE-2023-41772	CVE-2023-36582	CVE-2023-36712
CVE-2023-36566	CVE-2023-41771	CVE-2023-36583	CVE-2023-36713
CVE-2023-41763	CVE-2023-41770	CVE-2023-36584	CVE-2023-36729
CVE-2023-36414	CVE-2023-41768	CVE-2023-36585	CVE-2023-41774
CVE-2023-36561	CVE-2023-41767	CVE-2023-36589	CVE-2023-41769
CVE-2023-44487	CVE-2023-36743	CVE-2023-36590	CVE-2023-41766
CVE-2023-36780	CVE-2023-36776	CVE-2023-36591	CVE-2023-41765

CVE-2023-36789

CVE-2023-36786

CVE-2023-38159

CVE-2023-29348

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-36718: Vulnerabilidad crítica de ejecución remota de código en Microsoft Virtual Trusted Platform Module. CVSS: 6.8.

CVE-2023-41773, CVE-2023-41771, CVE-2023-41770, CVE-2023-41768, CVE-2023-41767, CVE-2023-38166, CVE-2023-41774, CVE-2023-41774, CVE-2023-41769, CVE-2023-41765: Vulnerabilidad crítica de ejecución remota de código en el Layer 2 Tunneling Protocol. CVSS: 7.1.

CVE-2023-35349: Vulnerabilidad crítica de ejecución remota de código en Microsoft Message Queuing. CVSS: 8.5.

CVE-2023-36697: Vulnerabilidad crítica de ejecución remota de código en Microsoft Message Queuing. CVSS: 5.9.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

.NET 6.0
.NET 7.0
ASP.NET Core 6.0
ASP.NET Core 7.0
Azure DevOps Server 2020.0.2
Azure DevOps Server 2020.1.2
Azure DevOps Server 2022.0.1
Azure HDInsight
Azure Identity SDK for .NET
Azure Identity SDK for Java
Azure Identity SDK for JavaScript
Azure Identity SDK for Python
Azure Network Watcher VM Extension
Azure RTOS GUIX Studio
Azure RTOS GUIX Studio Installer Application
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Common Data Model SDK for C#
Microsoft Common Data Model SDK for Java
Microsoft Common Data Model SDK for Python
Microsoft Common Data Model SDK for TypeScript

Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Exchange Server 2019 Cumulative Update 13
Microsoft ODBC Driver 17 for SQL Server on Linux
Microsoft ODBC Driver 17 for SQL Server on MacOS
Microsoft ODBC Driver 17 for SQL Server on Windows
Microsoft ODBC Driver 18 for SQL Server on Linux
Microsoft ODBC Driver 18 for SQL Server on MacOS
Microsoft ODBC Driver 18 for SQL Server on Windows
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office for Android
Microsoft Office for Universal
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft OLE DB Driver 18 for SQL Server
Microsoft OLE DB Driver 19 for SQL Server
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack
Microsoft SQL Server 2017 for x64-based Systems (CU 31)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (CU 22)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems (CU 8)
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.6
Microsoft Visual Studio 2022 version 17.7
Skype for Business Server 2015 CU13
Skype for Business Server 2019 CU7
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems

Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)

Enlaces

<https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36602>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36720>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36724>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36725>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36431>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36434>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36433>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36557>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36778>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36436>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36576>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36598>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36438>

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-2023-36563>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36722>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36569>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36570>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36731>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36732>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36566>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41763>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36414>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36561>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36780>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36420>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36568>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36721>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36417>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38171>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36418>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36419>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36730>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36429>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36717>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36718>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36726>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36737>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36415>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36416>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36723>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36728>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41773>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41772>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41771>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41770>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41768>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41767>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36743>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36776>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36790>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38166>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36435>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36902>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35349>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36785>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36564>

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-2023-36565>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36567>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36571>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36572>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36573>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36574>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36575>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36577>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36578>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36579>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36581>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36582>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36583>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36584>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36585>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36589>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36590>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36591>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36592>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36593>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36594>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36596>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36603>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36605>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36606>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36697>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36698>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36701>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36702>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36703>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36704>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36706>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36707>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36709>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36710>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36711>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36712>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36713>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36729>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41774>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41769>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41766>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41765>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36789>

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-2023-36786>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38159>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29348>