Alerta de seguridad cibernética	9VSA24-00976-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	13 de febrero de 2024
Última revisión	13 de febrero de 2024

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 las vulnerabilidades parchadas en la actualización de seguridad mensual de Microsoft, Update Tuesday, correspondiente a febrero de 2024.

Vulnerabilidades

CVE-2024-21315	CVE-2024-21370	CVE-2023-50387
CVE-2024-21420	CVE-2024-21368	CVE-2024-21304
CVE-2024-21404	CVE-2024-21366	CVE-2024-20673
CVE-2024-21380	CVE-2024-21365	CVE-2024-21413
CVE-2024-21410	CVE-2024-21362	CVE-2024-21405
CVE-2024-21412	CVE-2024-21361	CVE-2024-21401
CVE-2024-21406	CVE-2024-21360	CVE-2024-21374
CVE-2024-21386	CVE-2024-21359	CVE-2024-21328
CVE-2024-21384	CVE-2024-21358	CVE-2024-21393
CVE-2024-21378	CVE-2024-21357	CVE-2024-21403
CVE-2024-21377	CVE-2024-21356	CVE-2024-21395
CVE-2024-21381	CVE-2024-21353	CVE-2024-21327
CVE-2024-21389	CVE-2024-21352	CVE-2024-21391
CVE-2024-21364	CVE-2024-21351	CVE-2024-21379
CVE-2024-21376	CVE-2024-21350	CVE-2024-21372
CVE-2024-21402	CVE-2024-21349	CVE-2024-21369
CVE-2024-21397	CVE-2024-21348	CVE-2024-21367
CVE-2024-21396	CVE-2024-21347	CVE-2024-21363
CVE-2024-21394	CVE-2024-21340	CVE-2024-21346
CVE-2024-21375	CVE-2024-21339	CVE-2024-21345
CVE-2024-21371	CVE-2024-20684	CVE-2024-21344

CVE-2024-21343
CVE-2024-21342
CVE-2024-21341
CVE-2024-21338
CVE-2024-21329
CVE-2024-20667
CVE-2024-20695
CVE-2024-20679

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2024-21380: Vulnerabilidad de revelación de información en Microsoft Dynamics Business Central /NAV. CVSS: 8.0.

CVE-2024-21410: Vulnerabilidad de elevación de privilegios en Microsoft Exchange Server. CVSS: 9.8.

CVE-2024-21357: Vulnerabilidad de ejecución remota de código en Windows Pragmatic General Multicast (PGM). CVSS: 7.5.

CVE-2024-20684: Vulnerabilidad de denegación de servicio en Windows Hyper-V. CVSS: 6.4.

CVE-2024-21413: Vulnerabilidad de ejecución remota de código en Microsoft Outlook. CVSS: 9.8.

Mitigación

Implementar los parches correspondientes. Detalles y enlaces de descarga en https://msrc.microsoft.com/update-guide/.

Productos afectados

.NET 6.0
.NET 7.0
.NET 8.0
ASP.NET Core 6.0
ASP.NET Core 7.0
ASP.NET Core 8.0
Azure Connected Machine Agent
Azure DevOps Server 2019.1.2
Azure DevOps Server 2020.1.2
Azure DevOps Server 2022.1
Azure File Sync v14.0
Azure File Sync v15.0
Azure File Sync v16.0
Azure File Sync v17.0
Azure Kubernetes Service Confidential Containers
Azure Site Recovery
Azure Stack Hub
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems

Microsoft Azure Active Directory B2C
Microsoft Defender for Endpoint for Windows
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Dynamics 365 Business Central 2022 Release Wave 2
Microsoft Dynamics 365 Business Central 2023 Release Wave 1
Microsoft Dynamics 365 Business Central 2023 Release Wave 2
Microsoft Dynamics 365 Customer Engagement V9.1
Microsoft Entra Jira Single-Sign-On Plugin
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 13
Microsoft Exchange Server 2019 Cumulative Update 14
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft PowerPoint 2016 (32-bit edition)
Microsoft PowerPoint 2016 (64-bit edition)
Microsoft Publisher 2016 (32-bit edition)
Microsoft Publisher 2016 (64-bit edition)
Microsoft Teams for Android
Microsoft Visio 2016 (32-bit edition)
Microsoft Visio 2016 (64-bit edition)
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.6
Microsoft Visual Studio 2022 version 17.8
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Skype for Business 2016 (32-bit)
Skype for Business 2016 (64-bit)
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 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 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)
Windows Server 2022, 23H2 Edition (Server Core installation)

Enlaces

https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.13 17:09:53 -03'00'