Alerta de seguridad cibernética	9VSA23-00803-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	14 de marzo de 2023
Última revisión	14 de marzo 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 las vulnerabilidades parchadas en el Update Tuesday de Microsoft correspondiente a marzo de 2023.

Vulnerabilidades

CVE-2023-1017	CVE-2023-23402	CVE-2023-23422	CVE-2023-24876
CVE-2023-1018	CVE-2023-23403	CVE-2023-23423	CVE-2023-24879
CVE-2023-21708	CVE-2023-23404	CVE-2023-23618	CVE-2023-24880
CVE-2023-22490	CVE-2023-23405	CVE-2023-23946	CVE-2023-24882
CVE-2023-22743	CVE-2023-23406	CVE-2023-24856	CVE-2023-24890
CVE-2023-23383	CVE-2023-23407	CVE-2023-24857	CVE-2023-24891
CVE-2023-23385	CVE-2023-23408	CVE-2023-24858	CVE-2023-24892
CVE-2023-23388	CVE-2023-23409	CVE-2023-24859	CVE-2023-24906
CVE-2023-23389	CVE-2023-23410	CVE-2023-24861	CVE-2023-24907
CVE-2023-23391	CVE-2023-23411	CVE-2023-24862	CVE-2023-24908
CVE-2023-23392	CVE-2023-23412	CVE-2023-24863	CVE-2023-24909
CVE-2023-23393	CVE-2023-23413	CVE-2023-24864	CVE-2023-24910
CVE-2023-23394	CVE-2023-23414	CVE-2023-24865	CVE-2023-24911
CVE-2023-23395	CVE-2023-23415	CVE-2023-24866	CVE-2023-24913
CVE-2023-23396	CVE-2023-23416	CVE-2023-24867	CVE-2023-24919
CVE-2023-23397	CVE-2023-23417	CVE-2023-24868	CVE-2023-24920
CVE-2023-23398	CVE-2023-23418	CVE-2023-24869	CVE-2023-24921
CVE-2023-23399	CVE-2023-23419	CVE-2023-24870	CVE-2023-24922
CVE-2023-23400	CVE-2023-23420	CVE-2023-24871	CVE-2023-24923
CVE-2023-23401	CVE-2023-23421	CVE-2023-24872	CVE-2023-24930

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-1017 y CVE-2023-1018: Vulnerabilidades de elevación de privilegios en TPM2.0 Module Library.

CVE-2023-21708: Vulnerabilidad de ejecución remota de código al realizar una remote procedure call.

CVE-2023-23392: Vulnerabilidad de ejecución remota de código en HTTP Protocol Stack. Para explotarla, un atacante no autenticado necesitaría enviar una llamada RPC especialmente diseñada a un host RPC. Se recomienda bloquear el puerto TCP 135 en el firewall perimetral de la organización para reducir la probabilidad de recibir un ataque potencial a esta vulnerabilidad.

CVE-2023-23397: Vulnerabilidad de elevación de privilegios de Microsoft Outlook. Esta vulnerabilidad puede ser explotada por atacantes externos enviando emails especialmente diseñados que causen una conexión de la víctima con una ubicación UNC externa bajo el control de los atacantes.

Un atacante que explote exitosamente esta vulnerabilidad podría acceder al hash Net-NTLMv2 del usuario, que podría ser usado como base para un ataque de NTLM Relay contra otro servicio identificándose como el usuario.

CVE-2023-23404: Vulnerabilidad de ejecución remota de código en Windows Point-to-Point Tunneling Protocol.

CVE-2023-23411: Vulnerabilidad de denegación de servicio en Windows Hyper-V.

CVE-2023-23415: Vulnerabilidad de ejecución remota de código en Internet Control Message Protocol (ICMP).

CVE-2023-23416: Vulnerabilidad de ejecución remota de código en Windows Cryptographic Services.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Azure HDInsights
Azure Service Fabric 9.1 for Ubuntu
Azure Service Fabric 9.1 for Windows
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1

Microsoft Edge (Chromium-based)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Malware Protection Engine
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
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 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 Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.5
OneDrive for Android
OneDrive for iOS
OneDrive for MacOS Installer
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 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 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-Mar
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23383
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23385
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23388
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23389
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23391
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23392
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23393

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23394
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23395
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23396
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23397
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23398
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23401
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23402
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23403
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23404
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23405
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23406
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23407
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23408
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23409
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23410
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23411
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23412
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23413
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23414
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23416
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23418
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23422
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23423
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24856
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24862
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24863
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24864
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24865
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24866
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24867
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24869
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24870

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24872
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24876
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24879
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24880
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24882
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24892
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24921
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24930

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno
de Chile
Fecha: 2023.03.14
15:58:07 -03'00'