Alerta de seguridad cibernética	9VSA21-00493-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2021
Última revisión	14 de septiembre de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre 66 vulnerabilidades informadas Microsoft como parte de su Update Tuesday de septiembre.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-26434
CVE-2021-26435
CVE-2021-26436
CVE-2021-26437
CVE-2021-26439
CVE-2021-36930
CVE-2021-36952
CVE-2021-36954
CVE-2021-36955
CVE-2021-36956
CVE-2021-36959
CVE-2021-36960
CVE-2021-36961
CVE-2021-36962
CVE-2021-36963
CVE-2021-36964
CVE-2021-36965
CVE-2021-36966
CVE-2021-36967
CVE-2021-36968
CVE-2021-36969
CVE-2021-36972
CVE-2021-36973
CVE-2021-36974
CVE-2021-36975
CVE-2021-38624
CVE-2021-38625
CVE-2021-38626
CVE-2021-38628
CVE-2021-38629
CVE-2021-38630
CVE-2021-38632
CVE-2021-38633
CVE-2021-38634
CVE-2021-38635
CVE-2021-38636
CVE-2021-38637
CVE-2021-38638
CVE-2021-38639
CVE-2021-38641
CVE-2021-38642
CVE-2021-38644
CVE-2021-38645
CVE-2021-38646
CVE-2021-38647
CVE-2021-38648
CVE-2021-38649
CVE-2021-38650
CVE-2021-38651
CVE-2021-38652
CVE-2021-38653
CVE-2021-38654
CVE-2021-38655
CVE-2021-38656
CVE-2021-38657
CVE-2021-38658
CVE-2021-38659
CVE-2021-38660
CVE-2021-38661
CVE-2021-38667
CVE-2021-38669
CVE-2021-38671
CVE-2021-40440
CVE-2021-40444
CVE-2021-40447
CVE-2021-40448

Impactos

Vulnerabilidades Críticas

CVE-2021-26435: Vulnerabilidad de corrupción de memoria en Windows Scripting Engine. El ataque puede realizarse de forma remota y su explotación no requiere de autenticación, aunque requiere cierta interación de la víctima

CVE-2021-36965: Vulnerabilidad de ejecución remota de código en Windows WLAN AutoConfig Service. No requiere escalamiento de privilegios o interacción del usuario para ser explotada. WLAN AutoConfig Service es parte del mecanismo usado por Windows 10 para elegir redes inalámbricas a las cuales conectarse.

CVE-2021-38647: Vulnerabilidad de ejecución remota de código en Azure Open Management Infrastructure (OMI). Esta vulnerabilidad no requiere de privilegios ni de interacción del usuario, el atacante puede correr su código con tan solo enviar un mensaje especialmente diseñado al sistema afectado.

Productos Afectados

Accessibility Insights for Android
Azure Open Management Infrastructure
Azure Sphere
HEVC Video Extensions
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 Business Central 2020 Release Wave 2 – Update 17.10
Microsoft Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.5
Microsoft Edge (Chromium-based)
Microsoft Edge for Android
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 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 Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1

Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
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 2019 version 16.4 (includes 16.0 - 16.3)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
MPEG-2 Video Extension
Visual Studio Code
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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 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 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
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, version 2004 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://msrc.microsoft.com/update-guide
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26435
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26436
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36930
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38630
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38630

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38633
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38637
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38638
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38639
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38641
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38642
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38645
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38646
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38651
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38652
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38657
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38659
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38660
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38667
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38669
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38671
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40440
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40447
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40448

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.15 00:05:08 -03'00'