Alerta de seguridad cibernética	9VSA21-00504-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2021
Última revisión	13 de octubre 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 de vulnerabilidades en productos de Microsoft, compartidas por la compañía durante su actualización mensual de octubre.

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

Vulnerabilidades

CVE-2021-41346
CVE-2021-40474
CVE-2021-41345
CVE-2020-1971
CVE-2021-3449
CVE-2021-3450
CVE-2021-41361
CVE-2021-40479
CVE-2021-36953
CVE-2021-40455
CVE-2021-41347
CVE-2021-41354
CVE-2021-41352
CVE-2021-36970
CVE-2021-41363
CVE-2021-41350
CVE-2021-41348
CVE-2021-34453
CVE-2021-41355
CVE-2021-26427
CVE-2021-40457
CVE-2021-40481
CVE-2021-40480
CVE-2021-41344
CVE-2021-40484
CVE-2021-41343
CVE-2021-41342
CVE-2021-41357
CVE-2021-41353
CVE-2021-40471
CVE-2021-40472
CVE-2021-40454
CVE-2021-40485
CVE-2021-41340
CVE-2021-41339
CVE-2021-41338
CVE-2021-41337
CVE-2021-41336
CVE-2021-41335
CVE-2021-41334
CVE-2021-41332
CVE-2021-41331
CVE-2021-41330
CVE-2021-26442
CVE-2021-26441
CVE-2021-40489
CVE-2021-40488
CVE-2021-40487
CVE-2021-40486
CVE-2021-40483
CVE-2021-40482
CVE-2021-40478
CVE-2021-40477
CVE-2021-40476

CVE-2021-40475
CVE-2021-40469
CVE-2021-40470
CVE-2021-40467
CVE-2021-40466
CVE-2021-40465
CVE-2021-40468
CVE-2021-40463
CVE-2021-40464
CVE-2021-40462
CVE-2021-40460
CVE-2021-40461
CVE-2021-40456
CVE-2021-40473
CVE-2021-40449
CVE-2021-40450
CVE-2021-40443
CVE-2021-38672
CVE-2021-38663
CVE-2021-38662

Impactos

Riesgo crítico

CVE-2021-40486: Vulnerabilidad de tipo ejecución remota de código (RCE) que afecta a Microsoft Word, Office y algunas versiones de SharePoint Server y que puede ser explotada a través de Preview Pane. Requiere que un usuario abra un archivo especialmente diseñado, que puede ser enviado por email o a través de un sitio web.

CVE-2021-40461: Vulnerabilidad de tipo ejecución remota de código (RCE) que afecta a Windows Hyper-V. La vulnerabilidad permite que una máquina virtual pueda pasar de guest a host y leer memoria del kernel (nucleo).

CVE-2021-38672: Vulnerabilidad de tipo ejecución remota de código (RCE) que afecta a Windows Hyper-V. La vulnerabilidad permite que una máquina virtual pueda pasar de guest a host y leer memoria del kernel (nucleo).

Otras vunlerabilidades de riesgo importante

CVE-2021-40444: Vulnerabilidad de tipo ejecución remota de código (RCE) en MSHTML que afecta a Microsoft Windows **y que está siendo explotada**.

CVE-2021-40449: Vulnerabilidad de elevación de privilegios en Win32k. **Está siendo explotada** como parte de una campaña APT de APT IronHusky, de acuerdo con Kaspersky.

Productos Afectados

.NET 5.0
Intune management extension
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 Dynamics 365 Customer Engagement V9.0
Microsoft Dynamics 365 Customer Engagement V9.1
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 Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 21
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2019 Cumulative Update 10
Microsoft Exchange Server 2019 Cumulative Update 11
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 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 SharePoint Enterprise 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)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
System Center 2012 R2 Operations Manager
System Center 2016 Operations Manager
System Center 2019 Operations Manager
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 11 for ARM64-based Systems
Windows 11 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-2021-41346
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41345

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41361
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40455
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41354
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41352
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41363
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41350
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41348
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34453
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41355
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26427
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40457
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40481
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41344
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40484
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41343
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41342
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41357
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41353
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40471
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40485
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41339
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41338
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41337
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41336
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41335
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41334
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41332
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41331
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41330
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26442
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26441
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40488
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40487

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40486
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40483
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40482
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40477
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40475
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40464
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40462
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40460
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40456
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40443
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38672
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38663
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38662

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.14 10:35:50 -03'00'