Alerta de seguridad cibernética	9VSA21-00466-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2021
Última revisión	13 de julio 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 vulnerabilidades que afectan a diversos productos de Microsoft, parte de su Update Tuesday mensual.

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

Vulnerabilidades

CVE-2021-31183
CVE-2021-31196
CVE-2021-31206
CVE-2021-31947
CVE-2021-31961
CVE-2021-31979
CVE-2021-31984
CVE-2021-33740
CVE-2021-33743
CVE-2021-33744
CVE-2021-33745
CVE-2021-33746
CVE-2021-33749
CVE-2021-33750
CVE-2021-33751
CVE-2021-33752
CVE-2021-33753
CVE-2021-33754
CVE-2021-33755
CVE-2021-33756
CVE-2021-33757
CVE-2021-33758
CVE-2021-33759
CVE-2021-33760
CVE-2021-33761
CVE-2021-33763
CVE-2021-33764
CVE-2021-33765
CVE-2021-33766
CVE-2021-33767
CVE-2021-33768
CVE-2021-33771
CVE-2021-33772
CVE-2021-33773
CVE-2021-33774
CVE-2021-33775
CVE-2021-33776
CVE-2021-33777
CVE-2021-33778
CVE-2021-33779
CVE-2021-33780
CVE-2021-33781
CVE-2021-33782
CVE-2021-33783
CVE-2021-33784
CVE-2021-33785
CVE-2021-33786
CVE-2021-33788
CVE-2021-34438
CVE-2021-34439
CVE-2021-34440
CVE-2021-34441
CVE-2021-34442
CVE-2021-34444
CVE-2021-34445
CVE-2021-34446
CVE-2021-34447
CVE-2021-34448
CVE-2021-34449
CVE-2021-34450
CVE-2021-34451
CVE-2021-34452
CVE-2021-34454
CVE-2021-34455
CVE-2021-34456
CVE-2021-34457
CVE-2021-34458
CVE-2021-34459
CVE-2021-34460
CVE-2021-34461
CVE-2021-34462
CVE-2021-34464

CVE-2021-34466	CVE-2021-34489	CVE-2021-34501	CVE-2021-34516
CVE-2021-34467	CVE-2021-34490	CVE-2021-34503	CVE-2021-34517
CVE-2021-34468	CVE-2021-34491	CVE-2021-34504	CVE-2021-34518
CVE-2021-34469	CVE-2021-34492	CVE-2021-34507	CVE-2021-34519
CVE-2021-34470	CVE-2021-34493	CVE-2021-34508	CVE-2021-34520
CVE-2021-34473	CVE-2021-34494	CVE-2021-34509	CVE-2021-34521
CVE-2021-34474	CVE-2021-34496	CVE-2021-34510	CVE-2021-34522
CVE-2021-34476	CVE-2021-34497	CVE-2021-34511	CVE-2021-34523
CVE-2021-34477	CVE-2021-34498	CVE-2021-34512	CVE-2021-34525
CVE-2021-34479	CVE-2021-34499	CVE-2021-34513	CVE-2021-34528
CVE-2021-34488	CVE-2021-34500	CVE-2021-34514	CVE-2021-34529

Impactos

Microsoft considera como vulnerabilidades críticas las siguientes:

CVE-2021-33740	CVE-2021-34458	CVE-2021-34494
CVE-2021-34439	CVE-2021-34464	CVE-2021-34497
CVE-2021-34448	CVE-2021-34473	CVE-2021-34503
CVE-2021-34450	CVE-2021-34474	CVE-2021-34522

Algunas vulnerabilidades críticas destacables son:

CVE-2021-34448. Esta vulnerabilidad es de ejecución remota de código y afecta al scripting engine presente en cada versión de Windows aún con soporte.

CVE-2021-33771 y CVE-2021-31979 son vulnerabilidades de elevación de privilegios en el kernel de Windows, y están siendo explotadas.

CVE-2021-34458 es un error de ejecución remota de código en las áreas más profundas del sistema operativo.

CVE-2021-34494 es una vulnerabilidad en Windows DNS Server que alcanzó una clasificación CVSS de severidad de 9,8 de 10.

Junto a las nuevas vulnerabilidades, Microsoft también lanzó parches a vulnerabilidades ya reconocidas, incluyendo un parche actualizado a CVE-2021-34527, error popularmente conocido como PrintNightmare.

Productos Afectados

.NET Education Bundle SDK Install Tool
.NET Install Tool for Extension Authors
HEVC Video Extensions
Microsoft 365 Apps for Enterprise
Microsoft Bing Search for Android

Microsoft Dynamics 365 Business Central 2020
Microsoft Dynamics 365 Business Central 2021
Microsoft Excel 2013, 2013 RT, 2015
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2013, 2016, 2019
Microsoft Malware Protection Engine
Microsoft Office 2013, 2013 RT, 2016, 2019
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013
Microsoft SharePoint Enterprise Server 2013
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013
Microsoft SharePoint Server 2019
Microsoft Word 2016
Open Enclave SDK
Power BI Report Server
Visual Studio Code
Windows 10
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2004, 2008, 2012, 2012 R2, 2016, 2019, 20H2

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://msrc.microsoft.com/update-guide
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34448
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31954
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34521
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34458
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33771
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31196
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31206
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31947
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33746

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33753
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33755
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33756
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33771
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33773
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33781
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34440
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34441
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34442
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34445
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34446
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34447

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34448
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34451
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34452
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34454
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34455
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34456
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34457
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34458
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34459
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34460
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34462
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34464
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34477
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34488
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34493
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34494
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34497
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34498
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34499
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34500
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34501
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34503
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34504
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34507
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34511

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34519
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34520
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34522
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34523
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34529

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.13 23:47:45 -04'00'