Alerta de seguridad cibernética	9VSA21-00454-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2021
Última revisión	10 de junio 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 en diversos productos de Microsoft, cinco de ellas críticas.

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

Vulnerabilidades

CVE-2021-33739
CVE-2021-31985
CVE-2021-31978
CVE-2021-31957
CVE-2021-31959
CVE-2021-31971
CVE-2021-31980
CVE-2021-31977
CVE-2021-31976
CVE-2021-31975
CVE-2021-31974
CVE-2021-31973
CVE-2021-31972
CVE-2021-31970
CVE-2021-31968
CVE-2021-31969
CVE-2021-31967
CVE-2021-31966
CVE-2021-31965
CVE-2021-31964
CVE-2021-31963
CVE-2021-31950
CVE-2021-31949
CVE-2021-31948
CVE-2021-31944
CVE-2021-31943
CVE-2021-31942
CVE-2021-31941
CVE-2021-31940
CVE-2021-31939
CVE-2021-26420
CVE-2021-31983
CVE-2021-31946
CVE-2021-31945
CVE-2021-31955
CVE-2021-1675
CVE-2021-31952
CVE-2021-31958
CVE-2021-31960
CVE-2021-31956
CVE-2021-31954
CVE-2021-31201
CVE-2021-31199
CVE-2021-31951
CVE-2021-31953
CVE-2021-26414
CVE-2021-31962
CVE-2021-33742
CVE-2021-31938

Impactos

Cinco de las vulnerabilidades son consideradas críticas

CVE-2021-31985 es una vulnerabilidad crítica en el software antimalware Defender de Microsoft que permite la ejecución remota de código.

CVE-2021-31963 es una vulnerabilidad crítica en Microsoft SharePoint Server que permite la ejecución remota de código.

CVE-2021-31967 es una vulnerabilidad crítica en VP9 Video Extensions que permite la ejecución remota de código.

CVE-2021-31959 es una vulnerabilidad crítica en Windows que permite la ejecución remota de código.

CVE-2021-31942 es una vulnerabilidad crítica en Windows MSHTML Platform que permite la ejecución remota de código.

Productos Afectados

Microsoft Windows
.NET Core
Visual Studio
Microsoft Office
Microsoft Edge (Chromium-based y EdgeHTML)
Microsoft SharePoint Server
Hyper-V
Visual Studio Code – Kubernetes Tools
Windows HTML Platform
Windows Remote Desktop

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31985
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31959
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31967
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31963
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31957

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31949
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31948
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31944
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31940
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31939
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31945
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1675
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31201
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31199
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26414
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31938

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.10 12:41:49 -04'00'