Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00443-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2021
Última revisión	11 de mayo 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, CSIRT de Gobierno, comparte vulnerabilidades que afectan a distintos productos de Microsoft, correspondientes a su alerta de seguridad mensual (Update Tuesday).

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

Vulnerabilidades

CVE-2021-26419
CVE-2020-24588
CVE-2020-24587
CVE-2021-31204
CVE-2021-26422
CVE-2021-26421
CVE-2021-31936
CVE-2021-31214
CVE-2021-31213
CVE-2021-31211
CVE-2021-31209
CVE-2021-31200
CVE-2021-31208
CVE-2021-31207
CVE-2021-31205
CVE-2021-28465
CVE-2021-31198
CVE-2021-31195
CVE-2021-31194
CVE-2021-31193
CVE-2021-31192
CVE-2021-31191
CVE-2021-31190
CVE-2021-31188
CVE-2021-31187
CVE-2021-31186
CVE-2021-31185
CVE-2021-31184
CVE-2021-31182
CVE-2021-31181
CVE-2021-31180
CVE-2021-31179
CVE-2021-31178
CVE-2021-31177
CVE-2021-31176
CVE-2021-31175
CVE-2021-31174
CVE-2021-31173
CVE-2021-31172
CVE-2021-31171
CVE-2021-31170
CVE-2021-31169
CVE-2021-31168
CVE-2021-31167
CVE-2021-31166
CVE-2021-31165
CVE-2021-26418
CVE-2021-28479
CVE-2021-28478
CVE-2021-28476
CVE-2021-28474
CVE-2021-28461
CVE-2021-28455
CVE-2020-26144
CVE-2021-27068

Impactos

Microsoft considera como críticas las siguientes cuatro vulnerabilidades: CVE-2021-26419, CVE-2021-31194, CVE-2021-31166 y CVE-2021-28476.

CVE-2021-31194: Esta vulnerabilidad de ejecución remota de código en OLE Automation permite a un usuario con bajos privilegios comprometer un sistema resultando en una pérdida completa de integridad y disponibilidad del sistema y de la confidencialidad de los datos contenidos en él.

CVE-2021-31166: Esta vulnerabilidad relacionada con el protocolo HTTP permite a un atacante no autenticado a ejecutar código remoto, lo que podría ser aprovechado con un gusano.

CVE-2021-26419: Esta vulnerabilidad en Internet Explorer permite a un usuario remoto ejecutar código arbitrario en el sistema objetivo. Tiene lugar debido a un error de límites de la memoria. Su explotación exitosa puede acabar en el compromiso total del sistema.

CVE-2021-28476: Esta vulnerabilidad de ejecución remota de código en Hyper-V permite a un usuario con bajos privilegios comprometer un sistema resultando en una pérdida completa de integridad y disponibilidad del sistema y de la confidencialidad de los datos contenidos en él.

Como de severidad importante se listan las siguientes vulnerabilidades:

CVE-2020-24588	CVE-2021-28465	CVE-2021-31181	CVE-2021-31168
CVE-2020-24587	CVE-2021-31198	CVE-2021-31180	CVE-2021-31167
CVE-2021-31204	CVE-2021-31195	CVE-2021-31179	CVE-2021-31165
CVE-2021-26422	CVE-2021-31193	CVE-2021-31178	CVE-2021-26418
CVE-2021-26421	CVE-2021-31192	CVE-2021-31177	CVE-2021-28479
CVE-2021-31936	CVE-2021-31191	CVE-2021-31176	CVE-2021-28478
CVE-2021-31214	CVE-2021-31190	CVE-2021-31175	CVE-2021-28474
CVE-2021-31213	CVE-2021-31188	CVE-2021-31174	CVE-2021-28461
CVE-2021-31211	CVE-2021-31187	CVE-2021-31173	CVE-2021-28455
CVE-2021-31209	CVE-2021-31186	CVE-2021-31172	CVE-2020-26144
CVE-2021-31200	CVE-2021-31185	CVE-2021-31171	CVE-2021-27068
CVE-2021-31208	CVE-2021-31184	CVE-2021-31170	
CVE-2021-31205	CVE-2021-31182	CVE-2021-31169	

Productos Afectados

.NET 5.0
.NET Core 3.1
common_utils.py
Dynamics 365 for Finance and Operations
Internet Explorer 11
Internet Explorer 9
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Accessibility Insights for Web
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 19
Microsoft Exchange Server 2016 Cumulative Update 20
Microsoft Exchange Server 2019 Cumulative Update 8
Microsoft Exchange Server 2019 Cumulative Update 9
Microsoft Lync Server 2013 CU10
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 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)
Skype for Business Server 2015 CU11
Skype for Business Server 2019 CU5
Visual Studio 2019 for Mac version 8.9
Visual Studio Code
Visual Studio Code Remote - Containers Extension
Web Media Extensions
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 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 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 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, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)

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-2021-26419
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28476
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31166
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26418
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26422
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27068
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28455
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31165
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31166
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31167
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31168
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31170
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31171
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31172
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31173
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31174
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31175
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31178
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31179
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31180
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31184

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31185
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31186
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31187
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31188
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31190
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31191
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31192
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31195
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31198
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31200
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31204
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31205
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31207
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31209
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31213
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31214
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31936

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.11 18:13:18 -04'00'