



COMANDO DE
LAS FUERZAS
MILITARES



DIRECCIÓN GENERAL DE
TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

Departamento de
Ciberseguridad

BOLETÍN DE ALERTA

Boletín Número: 2021-11

Fecha de Publicación: 15/09/2021

Tema: Múltiples vulnerabilidades en productos de Microsoft.

SEVERIDAD: Crítica

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de Múltiples vulnerabilidades en productos de Microsoft.

El boletín mensual de septiembre de Microsoft detalla 86 vulnerabilidades, de las cuales 3 son de severidad crítica, 62 importantes, una moderada y 20 sin severidad asignada.

Recursos Afectados:

- Azure Open Management Infrastructure
- Azure Sphere
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Visual Studio

Departamento de Ciberseguridad

Dirección General de Tecnologías de la Información y Comunicación
Gral. Santos y Mcal. López - Edificio Comando FFMM - 2° Piso
ciberseguridadtic@ffmm.mil.py | +595 21 2498196
Asunción - Paraguay | www.digetic.mil.py



@DIGETIC



COMANDO DE
LAS FUERZAS
MILITARES



DIRECCIÓN GENERAL DE
TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

Departamento de
Ciberseguridad

- Windows Authenticode
- Windows Bitlocker
- Windows Installer
- Windows Kernel
- Windows MSHTML Platform
- Windows Print Spooler Components
- Windows Scripting
- Windows SMB
- Windows Update
- Windows Win32K
- Windows WLAN Auto Config Service
- Windows WLAN Service

Detalles:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos: ejecución remota de código, elevación de privilegios, denegación de servicio, omisión de características de seguridad, divulgación de información y suplantación de identidad (spoofing).

Mitigación:

En la mayor parte de los casos, el software afectado se actualizará automáticamente por defecto.

No obstante, en el caso de que no se realizase dicha actualización de forma automática, Microsoft pone a disposición de los usuarios un portal web con toda la información relacionada, así como los parches de los productos afectados para descarga y que se puede consultar aquí:

['Guía de actualizaciones de seguridad de Microsoft'](#).

Departamento de Ciberseguridad

Dirección General de Tecnologías de la Información y Comunicación
Gral. Santos y Mcal. López - Edificio Comando FFMM - 2° Piso
ciberseguridadtic@ffmm.mil.py | +595 21 2498196
Asunción - Paraguay | www.digetic.mil.py



@DIGETIC



COMANDO DE
LAS FUERZAS
MILITARES



DIRECCIÓN GENERAL DE
TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

Departamento de
Ciberseguridad

Se recomienda actualizar lo antes posible el software afectado a la última versión y [activar las actualizaciones automáticas](#) en caso de que no se estén aplicando por defecto.

Los usuarios que tengan instalados Windows 7, Windows Server 2008 R2 o Windows Server 2008 necesitan adquirir el Extended Security Update para seguir recibiendo las actualizaciones de seguridad.

Recuerda la importancia de mantener tus sistemas y aplicaciones siempre actualizados:

Referencia:

<https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep>

<https://msrc.microsoft.com/update-guide>

<https://support.microsoft.com/en-us/topic/security-update-deployment-information-september-14-2021-kb5005848-40a6ae09-aa00-497c-ba23-f4a62d7c813b>

<https://www.incibe.es/protege-tu-empresa/avisos-seguridad/boletin-mensual-microsft-septiembre-2021>

Departamento de Ciberseguridad

Dirección General de Tecnologías de la Información y Comunicación
Gral. Santos y Mcal. López - Edificio Comando FFMM - 2° Piso
ciberseguridadtic@ffmm.mil.py | +595 21 2498196
Asunción - Paraguay | www.digetic.mil.py



@DIGETIC