

Accesos corporativos

OTROS PORTALES



(<https://www.cert.org/>)



(<https://www.incibe.es/sites/default/files>)

(https://twitter.com/incibe_cert)

(<https://www.youtube.com/user/intecocert>)

/certificado_ens_incibe_3111219.pdf)

(<https://www.linkedin.com/showcase/incibe-cert>)



/certificado_sgsi_11112019.pdf)

(<https://www.incibe.es/sites/default/files>)



/certificado_sgc_13122019.pdf)



(<http://www.mineco.gob.es/>) funcionamiento y visualización de las estadísticas tal y como se recoge en la política de cookies en la columna "finalidad".

(<https://www.incibe.es/>)

continúa navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información.

Más información

[Política de cookies \(https://www.incibe.es/politica-cookies\)](https://www.incibe.es/politica-cookies) [Aceptar Cookies \(\)](#)

[Modificar su configuración \(https://www.incibe.es/politica-cookies#cookieconfig\)](https://www.incibe.es/politica-cookies#cookieconfig)

[Inicio \(/\)](#) / [Alerta Temprana](#) / [Vulnerabilidades \(/alerta-temprana/vulnerabilidades\)](#) / CVE-2019-0604 

Vulnerabilidad en Microsoft SharePoint (CVE-2019-0604)

Tipo: Validación incorrecta de entrada

Gravedad: Alta

Fecha publicación : 05/03/2019

Última modificación: 13/12/2019

Descripción

Existe una vulnerabilidad de ejecución remota de código en Microsoft SharePoint cuando el software no comprueba el marcado de origen de un paquete de una aplicación. Esto también se conoce como "Microsoft SharePoint Remote Code Execution Vulnerability". El ID de este CVE es diferente de CVE-2019-0594.

Impacto

Vector de acceso: A través de red

Complejidad de Acceso: Baja

Autenticación: No requerida para explotarla

Tipo de impacto: Afecta parcialmente a la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema

Productos y versiones vulnerables

- ◆ `cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*`
- ◆ `cpe:2.3:a:microsoft:sharepoint_server:2010:sp2:*:*:*:*`
- ◆ `cpe:2.3:a:microsoft:sharepoint_foundation:2013:sp1:*:*:*:*`
- ◆ `cpe:2.3:a:microsoft:sharepoint_enterprise_server:2016:*:*:*:*`

Para consultar la lista completa de productos y versiones ver [esta página](#)

Referencias a soluciones, herramientas e información

- ◆ [106914](#) (Origen: BID)
- ◆ <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604> (Origen: CONFIRM)

[Explicación de los campos \(/alerta-temprana/vulnerabilidades/ayuda-buscador-vulnerabilidades\)](#)

[◀ Ir atrás](#)

Este sitio web utiliza cookies propias y de terceros para el correcto funcionamiento y visualización del sitio web por parte del usuario, así como la recogida de estadísticas tal y como se recoge en la política de cookies en la columna "finalidad". !

continúa navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información.

[Política de cookies \(https://www.incibe.es/politica-cookies\)](https://www.incibe.es/politica-cookies) [Aceptar Cookies \(\)](#)

[Modificar su configuración \(https://www.incibe.es/politica-cookies#cookieconfig\)](https://www.incibe.es/politica-cookies#cookieconfig)



Este sitio web utiliza cookies propias y de terceros para el correcto funcionamiento y visualización del sitio web por parte del usuario, así como la recogida de estadísticas tal y como se recoge en la política de cookies en la columna "finalidad". **continúa navegando, consideramos que acepta su uso.** Puede cambiar la configuración u obtener más información.

[Política de cookies \(https://www.incibe.es/politica-cookies\)](https://www.incibe.es/politica-cookies) Aceptar Cookies ()

[Modificar su configuración \(https://www.incibe.es/politica-cookies#cookieconfig\)](https://www.incibe.es/politica-cookies#cookieconfig)