

Alerta de seguridad informática	9VSA20-00113-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2020
Última revisión	07 de Enero de 2020

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, comparte información obtenida de Microsoft, referente a una vulnerabilidad que afecta su herramienta de colaboración empresarial, Microsoft SharePoint. De ser explotada la vulnerabilidad, permitiría a un atacante remoto obtener información confidencial. El informe incluye la respectiva mitigación entregada por el proveedor.

Vulnerabilidad

CVE-2019-1491

Impacto

Esta vulnerabilidad permite a un atacante remoto realizar ataques de directorio transversal para obtener información confidencial. Esto es debido a un error de validación en la introducción de datos al procesar secuencias transversales de directorio.

Un atacante remoto y sin autenticación, podría enviar peticiones HTTP especialmente diseñadas al servidor SharePoint y lograr leer archivos arbitrarios del sistema.

Productos Afectados

Microsoft SharePoint Server 2016 y 2019.

Microsoft SharePoint Foundation: 2010 Service Pack 2, 2013 y 2013 Service Pack 1

Mitigación

Se deben aplicar las actualizaciones de seguridad publicadas por Microsoft en el enlace al final del documento.

Enlaces

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1491>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1491>