Alerta de seguridad cibernética	9VSA20-00347-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de diciembre de 2020
Última revisión	28 de diciembre 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 la información entregada por Google Project Zero por una vulnerabilidad que afecta al producto Windows de Microsoft.

Vulnerabilidad

CVE-2020-17008

Impacto

La vulnerabilidad CVE-2020-17008 es considerada de riesgo alto, ya que permite a un usuario local escalar privilegios en el sistema.

El origen de esta vulnerabilidad es una falla en la API de la cola de impresión splwow64.exe, que permite a un atacante ejecutar código arbitrario en el sistema, pudiendo instalar malware que cambie datos de las cuentas de usuario.

Esta vulnerabilidad existe por causa de un parche incompleto para la vulnerabilidad CVE-2020-0986, reportada originalmente en diciembre de 2019 y cuyo parche apareció en junio de 2020.

Productos afectados

Windows 8.1, 10 20H2, 10 1507 a 2004, 10 Gold, 10 Mobile, RT 8.1.

Windows Server 2021 a 2019 2004.

Mitigación

Aún no se conoce ninguna solución oficial para corregir esta vulnerabilidad. Microsoft espera entregar un parche en enero de 2021.

Enlaces

https://bugs.chromium.org/p/project-zero/issues/detail?id=2096

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17008