CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidades en Sistemas Windows

Fecha: **11/10/2022**

Problemática: **Múltiples vulnerabilidades en Microsoft Windows**

Correlativo: **AA-0040**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

Microsoft emitió un comunicado a través de sus canales oficiales informando sobre las múltiples vulnerabilidades en Sistemas Microsoft Windows, las mismas han sido identificadas como: CVE-2022-35840, CVE-2022-38004, CVE-2022-34727, CVE-2022-37969, CVE-2022-30170, CVE-2022-34724, CVE-2022-33647, CVE-2022-34732, CVE-2022-35830, CVE-20262-34, CVE-2022-34718, CVE-2022-34721, CVE-2022-37957, CVE-2022-37955, CVE-2022-34731, CVE-2022-35803, CVE-2022-30200, CVE-2022-34730, CVE-2022-34729, CVE-20062-38, CVE-2022-38005, CVE-2022-35831, CVE-2022-34723, CVE-2022-37959, CVE-2022-34725, CVE-2022-38011, CVE-2022-37956, CVE-2022-34733, CVE-2022-35836, CVE-8332-35, CVE-2022-35832, CVE-2022-37958, CVE-2022-35835, CVE-2022-33679, CVE-2022-26928, CVE-2022-37954, CVE-2022-34734, CVE-2022-34728, CVE-2022-23960, CVE-2022-35841, CVE-70202-34, CVE-2022-34719, CVE-2022-34722, CVE-2022-35837, CVE-2022-38019, CVE-2022-30196, CVE-2022-35838, CVE-2022-35834.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Se recomienda a los usuarios de sistemas Microsoft Windows a instalar las actualizaciones correspondientes desde la sección de Windows Update para mitigar las vulnerabilidades encontradas.

SITUACIÓN

De acuerdo a la información obtenida a raíz de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, la explotación de una o de las múltiples vulnerabilidades encontradas en sistemas Microsoft Windows, conllevaría a un ciberdelincuente a ejecutar código arbitrario, obtener privilegios, provocar la denegación de servicio, obtener información confidencial y eludir las restricciones de seguridad.

Productos afectados:

Microsoft Windows, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows 8, Windows RT, Microsoft Windows 10, Microsoft Azure, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows 11

DICCIONARIO DE DATOS

Ataque de fuerza bruta: Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
CVE: Acrónimo del inglés en Common Vulnerabilities and Exposures; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del software afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.
Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

REFERENCIAS

1. **https://threats.kaspersky.com/en/vulnerability/KLA19245/**
2. **https://conciber.gob.gt/?page_id=1208**
3. **https://msrc.microsoft.com/update-guide/vulnerability**

ÁREA PARA DEFINICIONES