Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°042	Fecha: 17-02-2024
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Descubierta una nueva vulnerabilidad de Microsoft Windows Defender que afecta a millones de usuarios		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES**:

   Trend Micro ha descubierto una vulnerabilidad en Microsoft Windows Defender que está siendo explotada activamente por el grupo de piratas informáticos Water Hydra. Ésta fue hallada el 31 de diciembre de 2023. Se aconseja a las organizaciones que tomen medidas inmediatas emitiendo parches virtuales.

2. **DETALLES:**

   Actualmente, esta vulnerabilidad está siendo activamente explotada por motivaciones financieras, con el objetivo de comprometer a los operadores de divisas que participan en el mercado de comercio de alto riesgo. Esta situación plantea una amenaza significativa tanto para la integridad de los datos como para la estabilidad financiera de las empresas afectadas.

   Específicamente, se utiliza en una sofisticada cadena de ataques de día cero para permitir una omisión de Windows Defender SmartScreen. Los ataques están diseñados para infectar a las víctimas con el troyano de acceso remoto (RAT) DarkMe para posibles robos de datos y ransomware.

   Utilizando capas de defensa para mitigar amenazas avanzadas, las capacidades del sistema de prevención de intrusiones (IPS) de Trend Micro entregaron parches virtuales a sus clientes para bloquear completamente la explotación de CVE-2024-21412. Se trata de identificar automáticamente las vulnerabilidades críticas y proporcionar visibilidad de todos los endpoints afectados y su posible impacto en el riesgo global de una organización.

3. **RECOMENDACIÓN:**

   - Actualizar el producto afectado a la última versión de software disponible que Cisco ha lanzado para abordar esta vulnerabilidad.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/encuentra-vulnerabilidad-zero-day-en-windows-defender_58092_102.html • hxxps://www.itdigitalsecurity.es/vulnerabilidades/2024/02/descubierta-una-nueva-vulnerabilidad-de-microsoft-windows-defender-que-afecta-a-millones-de-usuarios