DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 011**	**Fecha: 12-01-2023**
		Página 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Microsoft ha publicado actualizaciones de seguridad que corrige múltiples vulnerabilidades de severidad crítica		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Microsoft ha publicado actualizaciones de seguridad correspondiente al mes de enero 2023, que corrigen múltiples vulnerabilidades de severidad **CRÍTICA** y **ALTA** de tipo denegación de servicio, escalada de privilegios, divulgación de información, ejecución remota de código, omisión de características de seguridad y suplantación de identidad (spoofing) en varios de sus productos. Este paquete de actualizaciones corrige 98 vulnerabilidades de seguridad, incluida una vulnerabilidad que, según la compañía, se está explotando activamente en la naturaleza.

2. **Detalles:**

- Microsoft indicó que 11 de las 98 vulnerabilidades están clasificados como de severidad CRÍTICA y 87 están clasificados como ALTA, una de las vulnerabilidades también figura como conocida públicamente en el momento del lanzamiento. 39 de las vulnerabilidades que Microsoft cerró en esta actualización permite la elevación de privilegios.
- La actualización de enero corrige una serie de fallas de escalada de privilegios, incluida una en el Administrador de credenciales de Windows (CVE-2023-21726) y tres que afectan el componente Print Spooler (CVE-2023-21678, CVE-2023-21760 y CVE-2023-21765).
- Asimismo, Microsoft indicó que la vulnerabilidad que viene siendo explotado activamente en su naturaleza se relaciona con la registrada como CVE-2023-21674, una falla de escalada de privilegios en Windows Advanced Local Procedure Call (ALPC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante obtener permisos de SISTEMA. Esta vulnerabilidad podría conducir a un escape de la caja de arena del navegador, para ello, se requiere que un atacante ya haya obtenido una infección inicial en el host.
- Igualmente, Microsoft indicó también que otras dos vulnerabilidades de severidad alta de tipo escalada de privilegios identificadas que afectan a Microsoft Exchange Server (CVE-2023-21763 y CVE-2023-21764), que se derivan de un parche incompleto para CVE-2022-41123. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código con privilegios de nivel de SISTEMA al explotar una ruta de archivo codificada.
- Las actualizaciones emitidas llegan cuando Windows 7, Windows 8.1 y Windows RT llegaron al final del soporte el 10 de enero de 2023. La empresa indico que no ofrecerá un programa de actualización de seguridad extendida (ESU) para Windows 8.1, sino que exhortará a los usuarios a actualizar a Windows 11. Usar Windows 8.1 después del 10 de enero de 2023, puede aumentar la exposición de una organización a los riesgos de seguridad.

3. **Productos afectados:**

- Múltiples productos de Microsoft.