	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 033	Fecha: 07-02-2023
		Página 11 de 14

Componente que reporta	**CENTRO DE OPERACIONES CIBERESPACIALES**		
Nombre de la alerta	Ataques de ransomware aprovechando vulnerabilidad de VMware ESXi		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código malicioso		

Descripción

SITUACIÓN:

- Se tomó conocimiento de una campaña de ataques de ransomware (ataque que cifra la información de sistemas informáticos para luego pedir el pago de un rescate a cambio de devolver el acceso), estos ataques dirigidos al hipervisor ESXi, se están realizando explotando la vulnerabilidad CVE-2021-21974, la cual afecta el SLP (Protocolo de Ubicación del Servicio) y permite al atacante explotar el código arbitrario de forma remota.

- Se sospecha que las intrusiones están relacionadas con una nueva variante de ransomware basada en Rust llamada Nevada, registrándose ataques desde diciembre del 2022.

- Asimismo, se supo que estos ataques afectan las siguientes versiones:
  - Versiones de ESXi 7.x anteriores a ESXi70U1c-17325551
  - Versiones de ESXi 6.x anteriores a ESXi 6.7
  - Versiones de ESXi 6.7.x anteriores a ESXi670-202102401-SG
  - Versiones de ESXi 6.5.x anteriores a ESXi650-202102101-SG

RECOMENDACIONES:

- Se recomienda aplicar los parches disponibles para el hipervisor ESXi.
- Realizar un análisis del sistema para detectar cualquier signo de compromiso.
- Realizar copias de seguridad.
- Mantener el software actualizado.

Fuentes de información	▪ hxxps://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/