CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: **04/05/2024**

Problemática: **Fallo de Microsoft Outlook es aprovechado por ciberdelincuentes**

Correlativo: **AC-0021**

Institución / Sector: **Público y Privado**

CONTEXTO

República Checa y Alemania revelaron públicamente que fueron el objetivo de una campaña de ciberespionaje a largo plazo llevada a cabo por el actor de amenazas» vinculado a Rusia conocido como «APT28».

La falla de seguridad identidad como CVE-2023-23397, clasificada como crítica, permite al actor de amenazas escalar privilegios y acceder y secuestrar el directorio de hashes Net-NTLMv2 y luego emplearlos para autenticarse mediante un ataque de retransmisión.

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**

PRODUCTOS VULNERABLES

Microsoft Office
- **2019**
- **365**

RECOMENDACIONES

Ejecutar las actualizaciones recomendadas por el fabricante para corregir la falla presentada.

REFERENCIAS

The hacker News
https://thehackernews.com/2024/05/microsoft-outlook-flaw-exploited-by.html

Microsoft
https://answers.microsoft.com/es-es/msoffice/forum/all/como-mitigo-la-vulnerabilidad-cve-2023-23397-en/5d79f00f-6902-479c-8ce6-953aab7cdc4d