CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente informático

Fecha: 04/10/2023

Problemática: La web de la Casa Real británica sufre un ciberataque DDos

Correlativo: AC-0081

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Casa Real británica víctima de ciberataque que dejo inaccesible el servicio web de la institución.

SITUACIÓN

El ataque cibernético de tipo DDos (ataque distribuido de denegación de servicio) realizado por ciberdelincuentes dejo inaccesible temporalmente los servicios de la web,

Técnica: T1498
Subtécnicas: T1498.001 , T1498.002
Táctica: Impacto
Plataformas: Azure AD, Contenedores, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS
Tipo de Impacto: Disponibilidad

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	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

- Es necesario interceptar el tráfico entrante para filtrar el tráfico de ataque del tráfico legítimo
- Dependiendo del volumen de la inundación, el filtrado local puede ser posible bloqueando las direcciones de origen que originan el ataque, bloqueando los puertos a los que se dirige o bloqueando los protocolos que se utilizan para el transporte
- Analice el riesgo asociado a que los recursos críticos se vean afectados por ataques DoS de red y cree un plan de recuperación ante desastres/plan de continuidad

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.
- DDos (ataque distribuido de denegación de servicio): es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

REFERENCIAS

THE HACKER NEWS
https://thehackernews.com/2023/10/arm-issues-patch-for-mali-gpu-kernel.html

MITRE ATT&CK
https://attack.mitre.org/techniques/T1498/