

Vulnerabilidad de software

Fecha: 02/10/2023

Problemática: Google parchó vulnerabilidad crítica de Chrome

Correlativo: AC-0073

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Google lanzó parches de seguridad para corregir una falla de seguridad crítica en su navegador web Chrome que ha sido explotada y aprovechada por actores de amenazas.

SITUACIÓN

La falla CVE-2023-4863, se ha descrito como un caso de desbordamiento de búfer que reside en el formato de imagen WebP y que podría provocar la ejecución de código arbitrario o un bloqueo. La explotación exitosa de esta falla permitiría a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML diseñada.

Esta falla para ser aprovechada por un atacante y no necesita de otra para ejecutarse exitosamente.

Nivel de priorización

Prioridad
Urgente / No Urgente
Urgente

Actualización
Seguimiento/Preventiva/Resiliente
Preventiva

Matriz de Evaluación

| Riesgo Alto/ Medio/ Bajo | Nivel de Afectación | | |
|-----------------------------|---------------------|----------------|------------------|
| | Integridad | Disponibilidad | Confidencialidad |
| Alto | Alto | Alta | Alta |

RECOMENDACIONES

Ante esta problemática, se recomienda actualizar a la versión 116.0.5845.187/188 de Chrome para Windows y 116.0.5845.187 para macOS y Linux para mitigar posibles amenazas.

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.

REFERENCIAS

GOOGLE
<https://nvd.nist.gov/vuln/detail/CVE-2023-4863>