BOLETÍN DE ALERTA

Boletín Nro.: 2023-15
Fecha de publicación: 12/04/2023
Tema: Vulnerabilidades del tipo *out-of-bounds write* y *use-after-free (UAF*) en productos Apple

Producto afectado:

- iOS y iPadOS, versiones previas a 16.4.1.
- macOS Ventura, versiones previas a 13.3.1.
- Safari, versiones previas a 16.4.1.
- iPhone 8 y versiones posteriores.
- iPad Pro, todos los modelos.
- iPad Air 3ra generación y versiones posteriores.
- iPad 5ª generación y versiones posteriores.
- iPad mini 5ª generación y versiones posteriores.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre dos vulnerabilidades de día cero *(0-day*) explotadas activamente con (*PoC*) pública, que afectan a productos Apple, que permitirían a un atacante realizar ataques del tipo *use-after-free (UAF)*, *out-of-bounds write* y provocar la ejecución de código arbitrario en el sistema afectado.

Las vulnerabilidades reportadas se componen de 2 (dos) sin severidad ni puntuación asignada aún. Las mismas se detallan a continuación:

- CVE-2023-28205, sin severidad ni puntuación asignada aún. Esta vulnerabilidad de día cero (*0-day)* del tipo *use-after-free (UAF)* se debe a una falla en el procesamiento de contenido web del componente *WebKit* en productos Apple. Esto permitiría a un atacante a través de un sitio web especialmente diseñado provocar ejecución de código arbitrario en los productos afectados.

- CVE-2023-28206, sin severidad ni puntuación asignada aún. Esta vulnerabilidad de día cero (*0-day)* del tipo *out-of-bounds write* se debe a una falla de validación de datos de entradas del usuario en el componente *IOSurfaceAccelerator* en productos Apple. Esto permitiría a un atacante realizar ejecución de código arbitrario con privilegios de *kernel* en los productos afectados. Actualmente para esta vulnerabilidad existe una prueba de concepto (*PoC*) publicada en internet.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar ejecución de código arbitrario en los productos afectados.

Solución:

Recomendamos instalar la actualización correspondiente provista por el fabricante, mediante en el siguiente enlace:

- https://support.apple.com/en-us/HT201222

Información adicional:

- https://securityonline.info/apple-users-face-two-actively-exploited-0-day-cve-2023-28205-cve-2023-28206-flaws/
- https://securityonline.info/poc-for-0-day-cve-2023-28206-flaw-affecting-macos-ios-published/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28205
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28206
- https://support.apple.com/en-us/HT213721
- https://support.apple.com/en-us/HT213722
- https://support.apple.com/en-us/HT213720
- https://support.apple.com/en-us/HT201222