BOLETÍN DE ALERTA

Boletín Nro.: 2023-01
Fecha de publicación: 22/08/2023
Tema: Explotación activa de vulnerabilidad critica en productos de Trend Micro
Traffic Light Protocol (TLP): White

Producto afectado:

- Trend Micro Apex One On Premise (2019)
- Trend Micro Apex One as a Service
- Worry-Free Business Security 10.0 SP1
- Worry-Free Business Security Services (SaaS)

Descripción:

Se ha reportado una vulnerabilidad critica que afecta a productos Trend Micro denominada CVE-2023-41179 clasificada como critica con un puntaje de CVSS de 7.2. Dicha vulnerabilidad afecta específicamente al módulo de desinstalación del AV (desarrollado por terceros), dicho módulo esta contenido en Trend Micro Apex One (local y SaaS), Worry-Free Business Security y Worry-Free Business Security Services.

Existen indicios de que actualmente esta vulnerabilidad está siendo explotada activamente. La explotación de dicha vulnerabilidad podría permitir a un atacante manipular el módulo para ejecutar comandos arbitrarios en un sitio afectado. Es importante tener en cuenta que un atacante primero debe obtener acceso a la consola administrativa en el sistema de destino para poder explotar esta vulnerabilidad.

El equipo de investigación de Trend Micro, menciona en su *informe*, que “Trend Micro ha detectado al menos una instancia de un posible intento de explotación de CVE-2023-41179”. También enfatizó que "aunque el exploit puede requerir el cumplimiento de varias condiciones específicas, Trend Micro recomienda encarecidamente a los clientes que actualicen lo antes posible a las últimas versiones".

Impacto:

Una explotación exitosa de la falla podría permitir a un atacante manipular el componente para ejecutar comandos arbitrarios en la instalación afectada. Sin embargo, se requiere que el adversario ya tenga acceso a la consola administrativa en el sistema de destino.

Prevención:

Trend Micro ha lanzado parches que solucionan la vulnerabilidad. Se recomienda aplicar el parche lo antes posible.

- *Trend Micro Apex One On Premise (2019) SP1 Patch 1 (b12380)*
- *Worry-Free Business Security 10.0 SP1 Patch 2495*

Según Trend Micro, los problemas en Apex One as a Service ya se solucionaron en las actualizaciones del 31 de julio de 2023.

Información adicional:

- *https://www.helpnetsecurity.com/2023/09/21/cve-2023-41179/*
- *https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-41179*
- *https://nvd.nist.gov/vuln/detail/CVE-2023-41179*