Se descubrieron vulnerabilidades de seguridad de alta gravedad, que pasaron desapercibidas por varios años, en un controlador legítimo que forma parte de las soluciones antivirus de Avast y AVG.

> *«Estas vulnerabilidades permiten a los atacantes escalar privilegios que les permiten deshabilitar productos de seguridad, sobrescribir componentes del sistema, corromper el sistema operativo o realizar operaciones maliciosas sin obstáculos»,* dijo el investigador de SentinelOne, Kasif Dekel.

Rastreadas como CVE-2022-26522 y CVE-2022-26523, las vulnerabilidades residen en un controlador de kernel anti-rootkit legítimo llamado aswArPot.sys y se dice que se introdujeron en la versión 12.1 de Avast, que se lanzó en junio de 2016.

Específicamente, las vulnerabilidades tienen su origen en un controlador de conexión de socket en el controlador del kernel que podría conducir a una escalada de privilegios al ejecutar código en el kernel de un usuario para que no sea administrador, lo que podría causar que el sistema operativo se bloquee y muestre una pantalla azul de muerte (BSoD).

Preocupantemente, las vulnerabilidades también podrían explotarse como parte de un ataque de navegador de segunda etapa o para realizar un escape de sandbox, lo que tendría consecuencias de largo alcance.

Después de la divulgación responsable el 20 de diciembre de 2021, Avast abordó los problemas en la versión 22.1 del software lanzado el 8 de febrero de 2022. *«Se arregló el controlador BSoD del rootkit»*, dijo la compañía en sus notas de lanzamiento.

Aunque no existe evidencia de que se haya abusado de las fallas en la naturaleza, la revelación se produce pocos días después de que Trend Micro detallara un ataque de ransomware AvosLocker que aprovechó otro problema en el mismo controlador para finalizar las soluciones antivirus en el sistema comprometido.

Posteriormente, SentinelOne dijo que el error se remonta a la versión 12.1, que asegura que se lanzó en enero de 2012. Sin embargo, las mismas notas de la versión de Avast muestran que la versión 12.1 se envió en junio de 2016.