Se ha divulgado una vulnerabilidad de seguridad de alto impacto en el Agente de Control de N-Able que podría ser aprovechada por un atacante local sin privilegios para obtener permisos de SISTEMA.

Identificada como CVE-2023-27470 (puntuación CVSS: 8.8), el problema se relaciona con una vulnerabilidad de condición de carrera conocida como *«Tiempo de Comprobación a Tiempo de Uso»* (TOCTOU). Cuando se explota con éxito, esta vulnerabilidad podría ser utilizada para eliminar archivos arbitrarios en un sistema Windows.

La deficiencia de seguridad, que afecta a las versiones 7.0.41.1141 y anteriores, ha sido corregida en la versión 7.0.43, lanzada el 15 de marzo de 2023, tras una divulgación responsable realizada por Mandiant el 27 de febrero de 2023.

El concepto de *«Tiempo de Comprobación a Tiempo de Uso»* se refiere a una categoría de fallas de software en la que un programa verifica el estado de un recurso para un valor específico, pero dicho valor cambia antes de que el programa lo utilice, lo que anula efectivamente los resultados de la comprobación.

Explotar una falla de este tipo puede resultar en la pérdida de integridad y engañar al programa para que realice acciones que no debería realizar, lo que permite a un actor malintencionado acceder a recursos no autorizados.

Según la firma de inteligencia de amenazas propiedad de Google, CVE-2023-27470 se origina a partir de una condición de carrera TOCTOU en el Agente de Control (BASupSrvcUpdater.exe) al registrar múltiples eventos de eliminación de archivos (por ejemplo, archivos llamados aaa.txt y bbb.txt) y cada acción de eliminación en una carpeta específica llamada *«C:\ProgramData\GetSupportService_N-Central\PushUpdates.»*

> *«En términos simples, mientras BASupSrvcUpdater.exe registraba la eliminación de aaa.txt, un atacante podría rápidamente reemplazar el archivo bbb.txt con un enlace simbólico, redirigiendo el proceso hacia un archivo arbitrario en el sistema»*,

> explicó Andrew Oliveau, investigador de seguridad de Mandiant.

> *«Esta acción provocaría que el proceso eliminara archivos de manera no intencionada como NT AUTHORITY\SYSTEM.»*

Lo que es aún más preocupante es que esta eliminación arbitraria de archivos podría ser utilizada para obtener acceso a un Símbolo del Sistema elevado al aprovechar un ataque de condición de carrera que apunta a la funcionalidad de reversión del instalador de Windows, lo que podría conducir potencialmente a la ejecución de código.

> *«Las explotaciones de eliminación arbitraria de archivos ya no se limitan a ataques de denegación de servicio y pueden, de hecho, servir como un medio para lograr una ejecución de código elevada. Tales explotaciones pueden combinarse con la funcionalidad de reversión de MSI para introducir archivos arbitrarios en el sistema»*, señaló Oliveau

> *«Un proceso que en apariencia parece inofensivo de registro y eliminación de eventos dentro de una carpeta insegura puede permitir a un atacante crear pseudoenlaces simbólicos, engañando a procesos privilegiados para que realicen acciones en archivos no deseados.»*