CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: **18/12/2023**

Problemática: **Microsoft descubrió falla crítica en la función Perforce Helix Core Server**

Correlativo: **AC-0100**

Institución / Sector: **Público y Privado**

CONTEXTO

Microsoft descubrió cuatro vulnerabilidades en Perforce Helix Core Server, una plataforma de gestión de código fuente ampliamente utilizada por los sectores de juegos, gobierno, ejército y tecnología.

La vulnerabilidad «CVE-2023-45849», permite a atacantes no autenticados ejecutar código arbitrario como LocalSystem (una cuenta del sistema operativo Windows con privilegios elevados). En su configuración predeterminada, Perforce Server permite a atacantes no autenticados ejecutar de forma remota comandos arbitrarios, incluidos scripts de PowerShell, como LocalSystem.

Al aprovechar CVE-2023-45849, los atacantes pueden instalar puertas traseras, acceder a información confidencial, crear o modificar configuraciones del sistema y, potencialmente, tomar el control total del sistema que ejecuta una versión vulnerable de Perforce Server.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

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

IMPACTO

- CVE-2023-5759 (puntuación CVSS 7,5): DoS no autenticado a través del abuso del encabezado RPC.
- CVE-2023-45849 (puntuación CVSS 9,8): ejecución remota de código no autenticado como LocalSystem.
- CVE-2023-35767 (puntuación CVSS 7,5): DoS no autenticado mediante comando remoto.
- CVE-2023-45319 (puntuación CVSS 7,5): DoS no autenticado mediante comando remoto.

RECOMENDACIONES

- Restringir el acceso a Perforce Server a usuarios autenticados.
- Actualizar periódicamente el software de terceros.
- Seguir las recomendaciones dadas por fabricante para mitigar la falla.

REFERENCIAS

Fuente: Microsoft
https://www.bleepingcomputer.com/news/security/microsoft-discovers-critical-rce-flaw-in-perforce-helix-core-server/