Los investigadores de seguridad cibernética revelaron detalles sobre una vulnerabilidad de seguridad en la aplicación Netwrix Auditor, que de ser explotada con éxito, podría conducir a la ejecución de código arbitrario en los dispositivos afectados.

> *«Debido a que este servicio generalmente se ejecuta con amplios privilegios en un entorno de Active Directory, el atacante probablemente podría comprometer el dominio de Active Directory»*, dijo Bishop Fox en un aviso.

Auditor es una plataforma de auditoría y visibilidad que permite a las organizaciones tener una vista consolidada de sus entornos de TI, incluyendo Active Directory, Exchange, servidores de archivos, SharePoint, VMware y otros sistemas, todo desde una sola consola.

Netwrix, la compañía detrás del software, cuenta con más de 11,500 clientes en más de 100 países, como Airbus, Virgin, King´s College Hospital, Credissimo, entre otros.

La vulnerabilidad, que afecta a todas las versiones compatibles anteriores a la 10.5, se ha descrito como una deserialización de objetos inseguros, que ocurre cuando se analizan datos controlables por el usuario que no son de confianza para infligir ataques de ejecución remota de código.

La causa raíz del error es un servicio remoto .NET no seguro, al que se puede acceder en el puerto TCP 9004 en el servidor Netwrix, lo que permite que un atacante ejecute comandos arbitrarios en el servidor.

> *«debido a que el comando se ejecutó con privilegios NT AUTHORITY/SYSTEM, explotar este problema permitiría a un atacante comprometer completamente el servidor Netwrix»*, dijo Jordan Parkin, de Bishop Fox.

Se recomienda a las organizaciones que confían en Auditor que actualicen el software a la

última versión, 10.5, lanzada el pasado 6 de junio.