Citrix lanzó parches este martes para múltiples vulnerabilidades de seguridad nuevas, que afectan su servicio Citrix Endpoint Management (CEM), también conocido como XenMobile, un producto creado para empresas para ayudar a administrar y proteger los dispositivos móviles de sus empleados remotamente.

Citrix Endpoint Management ofrece a las empresas funciones de gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM). Permite a las compañías controlar qué aplicaciones pueden instalar sus empleados al tiempo que garantiza que se apliquen actualizaciones y configuraciones de seguridad para mantener protegida la información confidencial.

Según Citrix, hay un total de 5 vulnerabilidades que afectan las instancias locales de los servidores XenMobile que se utilizan en las empresas para administrar todas las aplicaciones, dispositivos o plataformas desde una ubicación central.

> *«Las remediaciones ya se han aplicado a las versiones en la nube, pero los usuarios de derechos híbridos deben aplicar las actualizaciones a cualquier instancia local»,* dijo la compañía.

En caso de que las vulnerabilidades sean explotadas exitosamente, podrían permitir que atacantes no autenticados obtengan privilegios administrativos en los servidores XenMobile afectados.

> *«Recomendamos que estas actualizaciones se realicen de inmediato. Si bien no hay exploits conocidos al momento de escribir este artículo, anticipamos que los actores malintencionados se moverán rápidamente para explotar»,* advirtió la compañía.

Las dos vulnerabilidades, rastreadas como CVE-2020-8208 y CVE-2020-8209, calificadas como críticas, afectan a las siguientes versiones de XenMobile Server:

- XenMobile Server 10.12 antes de RP2
- XenMobile Server 10.11 antes de RP4
- XenMobile Server 10.10 antes de RP6
- XenMobile Server 10.9 antes de RP5

La vulnerabilidad CVE-2020-8209, descubierta por Andrey Medov de Positive Technologies, podría permitir que un atacante no autenticado lea archivos arbitrarios fuera del directorio raíz del servidor web, incluidos archivos de configuración y claves de cifrado para datos confidenciales.

> *«La explotación de esta vulnerabilidad permite a los piratas informáticos obtener información que puede ser útil para violar el perímetro, ya que el archivo de configuración a menudo almacena las credenciales de la cuenta de dominio para el acceso LDAP»*, dijo Mendov.

Por lo tanto, con acceso a la cuenta de dominio, el atacante remoto puede apuntar a otros recursos externos de la empresa, como correo corporativo, VPN y aplicaciones web.

Pero algo peor, es que el atacante que logre leer el archivo de configuración, puede acceder a datos sensibles, como la contraseña de la base de datos (PostgreSQL local por defecto y una base de datos SQL Server remota en algunos casos).

Sin embargo, debido a que la base de datos se almacena dentro del perímetro corporativo y no se puede acceder desde el exterior, Mendov dijo que *«este vector de ataque solo se puede utilizar en ataques complejos, por ejemplo, con la participación de un cómplice interno».*

> *«Los últimos parches continuos que deben aplicarse para las versiones 10.9, 10.10, 10.11 y 10.12 están disponibles de inmediato»,* dijo Citrix en su blog.

> *«Cualquier versión anterior a la 10.9.x debe actualizarse a una versión compatible con el último parche continuo. Le recomendamos que actualice a la 10.12 RP3, la última versión compatible».*

Debido a que los productos Citrix han surgido recientemente como uno de los objetivos favoritos de los hackers después de la explotación salvaje de las vulnerabilidades de Citrix ADC, Gateway y Sharefile, se recomienda a los usuarios que parcheen sus sistemas con las últimas versiones del software.

Cabe mencionar que la compañía aún no ha revelado detalles técnicos de las vulnerabilidades, pero ya notificó previamente a varios CERT importantes en todo el mundo y a sus clientes el pasado 23 de julio.