Progress Software ha publicado actualizaciones de seguridad para corregir una grave vulnerabilidad en LoadMaster y en el hipervisor Multi-Tenant (MT) que podría permitir la ejecución de comandos arbitrarios en el sistema operativo.

Clasificada como CVE-2024-7591 (con una puntuación CVSS de 10.0), esta vulnerabilidad se ha descrito como un fallo de validación incorrecta de entrada, lo que conduce a la inyección de comandos en el sistema operativo.

> *«Atacantes remotos no autenticados que tengan acceso a la interfaz de administración de LoadMaster podrían enviar una solicitud http especialmente diseñada, lo que permitiría la ejecución de comandos arbitrarios en el sistema»*, explicó la empresa en un comunicado la semana pasada.
>
> *«Este problema ha sido resuelto mediante la sanitización de los datos ingresados por el usuario en las solicitudes, para evitar la ejecución de comandos arbitrarios en el sistema.»*

Las versiones afectadas por esta vulnerabilidad son las siguientes:

- LoadMaster (7.2.60.0 y todas las versiones anteriores)
- Hipervisor Multi-Tenant (7.1.35.11 y todas las versiones anteriores)

El investigador de seguridad Florian Grunow ha sido reconocido por el descubrimiento y reporte de esta vulnerabilidad. Progress indicó que no ha encontrado pruebas de que este fallo haya sido explotado en ataques reales.

Aun así, se aconseja a los usuarios aplicar las correcciones más recientes lo antes posible descargando un paquete adicional. La actualización puede realizarse accediendo a Configuración del Sistema > Administración del Sistema > Actualizar Software.

> *«Recomendamos a todos nuestros clientes que actualicen sus implementaciones de LoadMaster cuanto antes para fortalecer la seguridad de sus entornos. También sugerimos encarecidamente que sigan nuestras recomendaciones para mejorar la seguridad*«, indicó la empresa.