مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Progress Kemp LoadMaster

Tracking #:432316529

Date:19-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical OS command injection vulnerability, has been discovered in the Progress Kemp LoadMaster application that allows remote code execution on the underlying system.

TECHNICAL DETAILS:

A critical OS command injection vulnerability, identified as CVE-2024-1212, has been discovered in the Progress Kemp LoadMaster application delivery controller (ADC). This vulnerability allows an attacker to inject arbitrary operating system commands via the LoadMaster's web interface, potentially leading to remote code execution on the underlying system. This vulnerability is being actively exploited in the wild.

Vulnerability Details:

- **CVE-2024-1212** LoadMaster Pre-Authenticated OS Command Injection
- Severity 10.0, CRITICAL
- Unauthenticated remote attackers can access the system through the LoadMaster management interface, enabling arbitrary system command execution.

Affected Products:

- affected from 7.2.48.1 before 7.2.48.10
- affected from 7.2.54.0 before 7.2.54.8
- affected from 7.2.55.0 before 7.2.59.2

Fixed Versions:

- LMOS 7.2.59.2, 7.2.54.8, 7.2.48.10

RECOMMENDATIONS:

- Apply the latest available firmware patches for Progress Kemp LoadMaster as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.kemptechnologies.com/hc/en-us/articles/24325072850573-Release-Notice-LMOS-7-2-59-2-7-2-54-8-7-2-48-10-CVE-2024-1212