مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Progress Software

Tracking #:432318261

Date:16-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Progress Software has released security updates addressing two high-severity UI and API command injection vulnerabilities affecting LoadMaster load balancers and MOVEit Web Application Firewalls (WAF).

TECHNICAL DETAILS:

Progress Software has released security updates addressing two high-severity UI and API command injection vulnerabilities affecting LoadMaster load balancers and MOVEit Web Application Firewalls (WAF). Successful exploitation could allow a remote attacker to execute arbitrary system commands and potentially gain full control of the affected appliance.

Vulnerability Details

- **CVE-2025-13444 – CVSS 8.4 (High)**
  This vulnerability is caused by improper input validation in the UI and API related to the getcipherset command. A remote attacker could exploit this flaw by sending specially crafted requests, resulting in arbitrary command execution on the underlying system.
- **CVE-2025-13447 – CVSS 8.4 (High)**
  This vulnerability affects multiple administrative UI and API commands, including addapikey, delapikey, delcert, dmidecode, listapikeys, and ssodomain. Successful exploitation could allow an attacker to inject and execute system commands remotely.

Impact:
Exploitation of this vulnerability may lead to remote code execution with administrative privileges, enabling full compromise of the affected appliance.

Affected Products

- Progress LoadMaster
- Progress LoadMaster Long-Term Support Firmware (LTSF)
- Progress Multi-Tenant LoadMaster (Hypervisor / Manager Node)
- Progress MOVEit Web Application Firewall (WAF)

Fixed Versions

- LoadMaster GA: Upgrade to version 7.2.62.2
- LoadMaster LTSF: Upgrade to version 7.2.54.16
- Multi-Tenant LoadMaster Hypervisor: Upgrade to version 7.1.35.15
- MOVEit WAF: Upgrade to version 7.2.62.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Progress.

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://nvd.nist.gov/vuln/detail/CVE-2025-13447
- https://nvd.nist.gov/vuln/detail/CVE-2025-13444