

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in Progress OpenEdge AdminServer
Tracking #:432317676
Date:08-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Progress Software has released security updates to address a high-severity vulnerability in the OpenEdge AdminServer component.

TECHNICAL DETAILS:

Progress Software has released security updates addressing a high-severity vulnerability in the OpenEdge AdminServer component. The flaw, tracked as CVE-2025-7388, allows Remote Command Execution (RCE) via the Java RMI interface.

Since AdminServer typically runs with elevated privileges, successful exploitation may allow attackers to manipulate configuration properties and execute arbitrary operating system commands on affected systems.

Vulnerability Details

- **CVE-2025-7388**
- CVSS Score 8.4 High
- The OpenEdge AdminServer component uses Java RMI for remote administrative operations. This vulnerability arises from improper handling of the workDir parameter passed as the -w jvmStart argument. Quoted strings were not properly sanitized, enabling attackers to inject OS commands by manipulating quotation marks.
- Key risk factors include:
 - Remote exploitation: Exposed RMI stubs can be abused for RCE.
 - Privilege impact: AdminServer usually runs with elevated rights.
 - Downstream risk: Unauthorized RMI requests can invoke insecure operations.

Affected Versions:

- OpenEdge 12.2.17 and earlier, 12.8.8 and earlier.

Fixed Versions:

- OpenEdge LTS 12.2.18, OpenEdge LTS 12.8.9.

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-2025-7388>