



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Vulnerability in Progress Software OpenEdge platform**

Tracking #:432315702

Date:15-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Progress Software OpenEdge platform that could be exploited to gain unauthorized access to vulnerable systems.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-1403**
- CVSS Base Score: **10.0 CRITICAL**
- An authentication bypass vulnerability exists in OpenEdge Authentication Gateway and AdminServer on all platforms supported by the OpenEdge product. This vulnerability allows attackers to bypass authentication due to improper handling of usernames and passwords. Specifically, certain unexpected content within the credentials can lead to unauthorized access.
- Successful exploitation of this vulnerability could grant attackers unauthorized access to affected systems, potentially leading to further attacks such as data theft and deployment of malicious applications.
- Proof-of-concept (PoC) exploit code is publicly available.

### Affected Products:

Progress Software OpenEdge versions:

- 11.7.18 and earlier
- 12.2.13 and earlier
- 12.8.0

### Fixed Versions:

Progress Software OpenEdge versions:

- 11.7.19 (LTS Update)
- 12.2.14
- 12.8.1

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Progress Software.

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://community.progress.com/s/article/Important-Critical-Alert-for-OpenEdge-Authentication-Gateway-and-AdminServer>