مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE chain Vulnerability in Progress Telerik Report Server

Tracking #:432315919

Date:04-06-2024

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 INTELLGIENCE 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 Remote Code Execution (RCE)chain vulnerability in the Progress Telerik Report Server that allows an attacker to bypass authentication controls and execute arbitrary code on the server.

TECHNICAL DETAILS:

The Progress Telerik Report Server has been found to be vulnerable to a pre-authenticated remote code execution (RCE) chain, consisting of an authentication bypass vulnerability (CVE-2024-4358) and a deserialization issue (CVE-2024-1800).

- **CVE-2024-4358**-9.8 Critical- In Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier, on IIS, an unauthenticated attacker can gain access to Telerik Report Server restricted functionality via an authentication bypass vulnerability.
- **CVE-2024-1800**- 9.9 Critical- In Progress Telerik Report Server versions prior to 2024 Q1 (10.0.24.130), a remote code execution attack is possible through an insecure deserialization vulnerability.

Patched Version:

- Update to 2024 Q2 (10.1.24.514)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released for Progress Telerik Report Server.

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:

1. https://nvd.nist.gov/vuln/detail/CVE-2024-1800
2. https://nvd.nist.gov/vuln/detail/CVE-2024-4358