CYBER ADVISORY

TLP:CLEAR
30 May 2024

Progress Telerik Vulnerability

CVE-2024-4358 | Telerik | Authentication Bypass | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-4358.[1] The vulnerability affects Progress' Telerik Report Server versions up to and including 2024 Q1 (10.0.24.305).[2] Exploitation of the vulnerability may allow an attacker to bypass authentication controls, potentially accessing sensitive report data and server functionalities. Such access could lead to further exploitative actions within the network.[3]

The Cal-CSIC recommends immediately upgrading to Telerik Report Server 2024 Q2 (10.1.24.514).

For further information on upgrading the Telerik Report Server, please refer to Telerik Report Server Implementer Guide.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Tenable; "CVE-2024-4358;" https://www.tenable.com/cve/CVE-2024-4358; accessed 30 May 2024
[2] SOC Radar; "Progress Telerik Report Server Receives Security Update for Critical Auth Bypass Vulnerability, CVE-2024-4358;" https://socradar.io/progress-telerik-report-server-receives-security-update-for-critical-auth-bypass-vulnerability-cve-2024-4358/; accessed 30 May 2024
[3] Telerik Report Server; "Authentication Bypass Vulnerability;" https://docs.telerik.com/report-server/knowledge-base/registration-auth-bypass-cve-2024-4358; accessed 30 May 2024