*CYBER ADVISORY*

TLP:CLEAR
25 JUL 2024

# Telerik Insecure Deserialization Vulnerability

Telerik | CVE-2024-6327 | Remote Code Execution | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability affecting Telerik Report Server versions 2024 Q2 (10.1.24.514) and below, known as CVE-2024-6327.[1] Exploitation of this vulnerability could provide an attacker remote code execution (RCE) by deserializing untrusted data without sufficiently verifying the resulting data will be valid.[2]

| Affected Product | Issues | CVE Identifier(s) | CVSS v3.1 score |
|---|---|---|---|
| Telerik Report Server versions 2024 Q2 (10.1.24.514) or earlier | Remote code execution attack is possible through an insecure deserialization vulnerability. | CVE-2024-6327 | 9.9 Critical |

**Table 1: Vulnerable Telerik Products [3]**

The Cal-CSIC recommends immediately upgrading all affected Telerik Report Server to 2024 Q2 (10.1.24.709).

For further information on upgrading affected Telerik Report Server products, please refer to Telerik | Upgarding Report Server.

## 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] Bleeping Computer "Progress warns of critical RCE bug in Telerik Report Server;" https://www.bleepingcomputer.com/news/security/progress-warns-of-critical-rce-bug-in-telerik-report-server/; accessed 25 July 2024

[2] CVE Details; "CVE-2024-6327;" https://www.cve.org/CVERecord?id=CVE-2024-6327; accessed 25 July 2024

[3] Telerik Report Server; "Insecure Deserialization Vulnerability;" https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-6327; access 25 July 2024