



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



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 | Upgrading Report Server](#).

CAL-CSIC-202407-008

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

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

CAL-CSIC-202407-008

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR