

CVE-2024-4358

Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability

Exigent CISA KEV since Jun 13, 2024 Actively exploited Public exploit module (Metasploit)

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.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.975 99.9th percentile · FIRST	CISA DEADLINE Jul 4, 2024 KEV since 2024 · listed over a year
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.975 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
report server 2024	≤ 10.0.24.305	after 10.0.24.305	NVD

Sources

Vendor guidance	docs.telerik.com/report-server/knowledge-base/registration-auth-bypass-cve-2024-4358	NVD	nvd.nist.gov/vuln/detail/CVE-2024-4358
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-43994
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-4358		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.