Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Remote Code Execution Flaw Exposed in Progress Telerik Report Server

Date of Publication	Admiralty Code	TA Number
July 26, 2024	A1	TA2024287

Summary

First Seen: July 2024
Affected Products: Progress Telerik Report Server
Impact: Progress Software has addressed a significant remote code execution vulnerability in Telerik Report Server, identified as CVE-2024-6327, with a CVSS score of 9.9. This critical vulnerability could be exploited by remote attackers to execute arbitrary code on vulnerable systems, posing a serious risk to businesses using the affected software.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-6327	Progress Telerik Report Server Remote Code Execution Vulnerability	Progress Telerik Report Server	✗	✗	✓

Vulnerability Details

#1 Progress Software is urging Telerik Report Server customers to upgrade their systems due to a critical security vulnerability that could lead to remote code execution. This flaw, identified as CVE-2024-6327, affects Report Server versions up to 2024 Q2 (10.1.24.514) and has been assigned a CVSS score of 9.9, indicating its critical severity.

#2 The vulnerability stems from the deserialization of untrusted data, a process where unverified data is converted back into objects. When an application fails to adequately validate this data, attackers can exploit it to execute arbitrary code on unpatched systems. This creates a substantial risk for businesses using the affected software, as it allows remote attackers to compromise vulnerable systems and potentially cause significant security breaches.

#3

In June, security researchers discovered that by combining two vulnerabilities, CVE-2024-1800 and CVE-2024-4358, on Telerik Report Servers, they could achieve unauthenticated remote code execution. Notably, CVE-2024-1800 involves a deserialization flaw, which is particularly concerning. Although CVE-2024-6327 has not yet been exploited in the wild, the potential impact of this vulnerability, along with the recent exploitation of similar issues, highlights the urgent need for proactive mitigation measures.

#4

Progress Software has addressed the issue in version 10.1.24.709. As an interim mitigation measure, it is recommended to configure the Report Server Application Pool to run under an account with reduced permissions, thereby limiting the potential damage from an exploit.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6327	Progress Telerik Report Server versions before 2024 Q2 (10.1.24.709)	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*	CWE-502

Recommendations

Update: To mitigate the risk posed by CVE-2024-6327 vulnerability, update to Report Server 2024 Q2 (10.1.24.709) or later. Users are strongly advised to update to this version to reduce the risk of exploitation.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	

Patch Details

To mitigate the risk by CVE-2024-6327 vulnerability, update to Report Server 2024 Q2 (10.1.24.709) or later. Users are highly advised to update to the most recent version to ensure protection against this critical security flaw.

Link: https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-6327

References

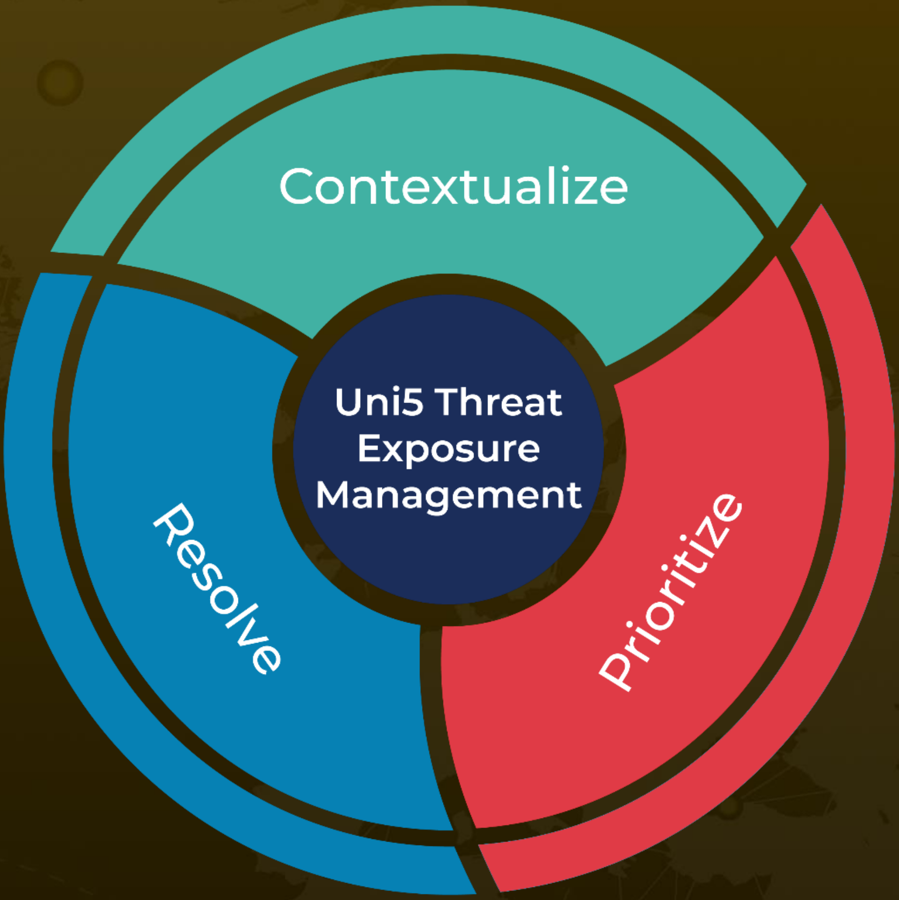
https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-6327

https://hivepro.com/threat-advisory/chained-flaws-in-progress-telerik-report-server-enable-unauthenticated-rce/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 26, 2024 • 6:30 AM

More at www.hivepro.com