Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Chained Flaws in Progress Telerik Report Server Enable Unauthenticated RCE

Date of Publication	Admiralty Code	TA Number
June 04, 2024	A1	TA2024214

Summary

Discovered: April 25, 2024
Affected Products: Progress Telerik Report Servers
Impact: A proof-of-concept (PoC) exploit script has been publicly disclosed, demonstrating a chained remote code execution (RCE) vulnerability present in Progress Telerik Report Servers. This exploit leverages two vulnerabilities, CVE-2024-1800 and CVE-2024-4358, an authentication bypass, and a deserialization flaw, respectively, to execute arbitrary code on the target system.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-1800	Progress Telerik Report Server Insecure Deserialization Vulnerability	Progress Telerik Report Server	✗	✗	✓
CVE-2024-4358	Progress Telerik Report Server Authentication Bypass Vulnerability	Progress Telerik Report Server	✗	✗	✓

Vulnerability Details

#1 A chained remote code execution (RCE) vulnerability on Progress Telerik Report Servers has been demonstrated through a publicly available proof-of-concept (PoC) exploit script. This exploit leverages two vulnerabilities—an authentication bypass (CVE-2024-1800) and a deserialization issue (CVE-2024-4358)—to execute code on the target system.

#2 CVE-2024-1800 arises from flawed input validation in the ObjectReader class, enabling attackers to send carefully crafted data that can trigger arbitrary code execution, potentially resulting in a complete system takeover.

#3 CVE-2024-4358 affects Progress Telerik Report Server versions up to 2024 Q1 (10.0.24.305) running on IIS. It enables unauthenticated attackers to bypass authentication mechanisms, granting them access to restricted functionalities, such as creating admin accounts without proper authorization checks.

#4 By exploiting CVE-2024-4358 and CVE-2024-1800, attackers can utilize the 'Register' method in the 'StartupController' to create admin accounts without authentication. Additionally, attackers can trigger the custom deserializer in Telerik Report Server using a specially crafted XML payload containing a 'ResourceDictionary' element. This deserializer interprets XML elements into .NET types, allowing execution of arbitrary commands on the server via the payload.

#5 Organizations are strongly urged to apply the available updates promptly, specifically upgrading to version 10.1.24.514 or later, as these updates address both vulnerabilities. Additionally, the vendor recommends that system administrators review their Report Server's user list for any unfamiliar new Local users added at '{host}/Users/Index,' despite no reported instances of active exploitation of CVE-2024-4358.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-1800	Progress Telerik Report Server versions prior to 2024 Q1 (10.0.24.130)	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	CWE-502
CVE-2024-4358	Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	CWE-290

Recommendations

Update: Admins are advised to update their Report Server 2024 Q2 (10.1.24.514) or later to mitigate the risk of exploitation of these and other vulnerabilities.

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.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	**T1136** Create Account	**T1068** Exploitation for Privilege Escalation	

Patch Details

Organizations must promptly apply the available updates, specifically upgrading to version 10.1.24.514 or later, which addresses both flaws.

Links:
https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

References

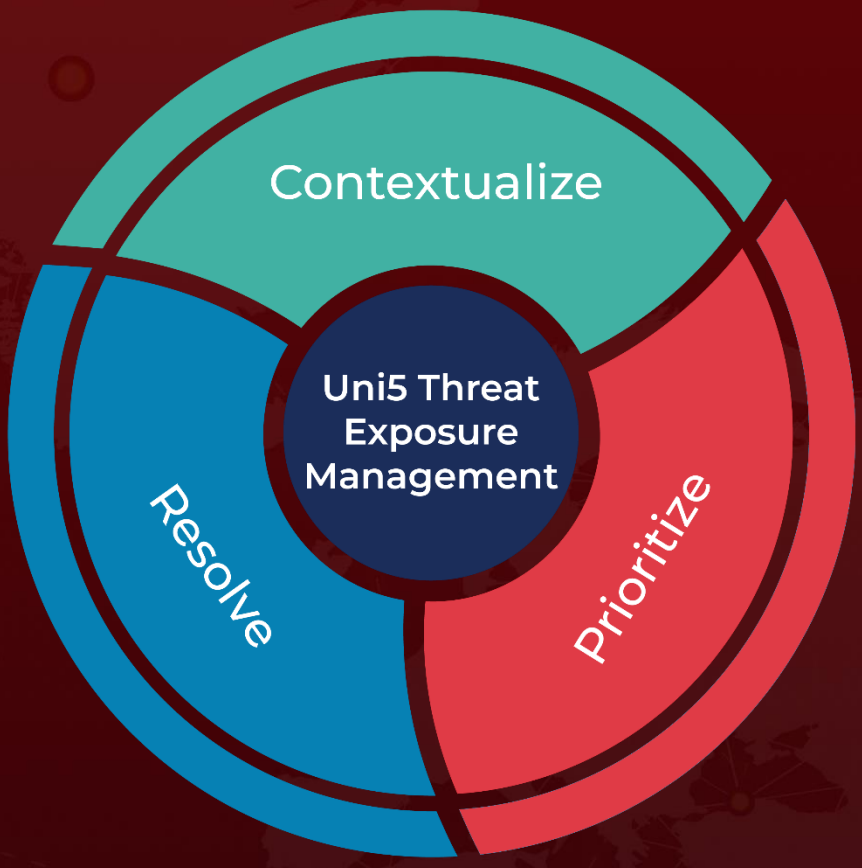
https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-1800

https://docs.telerik.com/report-server/knowledge-base/registration-auth-bypass-cve-2024-4358

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

June 04, 2024 • 6:30 AM

More at www.hivepro.com