June 14, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of an exploit chain involving two vulnerabilities in Progress Telerik Report Server. The vulnerability affects versions Progress Telerik Report Server prior to 2024 Q2 (10.1.24.514).

Technical Details

An insecure deserialization vulnerability in Progress' Telerik Report Server, was found in the ObjectReader class and is caused by improper validation of user-supplied input. When exploited, an attacker could execute code as the SYSTEM user.

Additionally, there is an authentication bypass vulnerability in Progress' Telerik Report Server, the flaw exists due to a lack of validation of the current installation step in the Register method.

By combining the authentication bypass flaw (CVE-2024-4358) with the previously disclosed insecure deserialization vulnerability (CVE-2024-1800) as part of an exploit chain to create a malicious report, an attacker could execute arbitrary code on a vulnerable Progress Telerik Report Server.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-4358, CVE-2024-1800
- Authentication Bypass Vulnerability
- Insecure Deserialization Vulnerability
- CVE-2024-4358, CVE-2024-1800: Exploit Code Available for Critical Exploit Chain in Progress Telerik Report Server
- VRM Vulnerability Reports