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 a new security issue was discovered that affects the JetBrains GitHub plugin on the IntelliJ Platform. The vulnerability affects versions prior to Aqua: 2024.1.2; CLion: 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip: 2024.1.4; DataSpell: 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2; GoLand: 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; IntelliJ IDEA: 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS: 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm: 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm: 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider: 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine: 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover: 2024.1.1; and WebStorm: 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4.

Technical Details

An external security report with details of a possible vulnerability that would affect pull requests within the IDE has been released. In particular, malicious content as part of a pull request to a GitHub project which would be handled by IntelliJ-based IDEs, would expose access tokens to a third-party host. The CVE ID assigned to this vulnerability is CVE-2024-37051.

Furthermore, if you have actively used GitHub pull request functionality in the IDE, it is advised that you revoke any GitHub tokens being used by the plugin. Given that the plugin can use OAuth integration or Personal Access Token (PAT), please check both and revoke as necessary.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required

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-2024-37051
- Fixed security issues
- Updates for security issue affecting IntelliJ-based IDEs 2023.1+ and JetBrains GitHub Plugin
- VRM Vulnerability Reports