Security Advisory 2024-057

Vulnerabilities in JetBrains Products

June 12, 2024 — v1.0

TLP:CLEAR

History:

- *12/06/2024 — v1.0 – Initial publication*

Summary

On June 10, JetBrains released a fix for a vulnerability affecting IntelliJ-based IDEs 2023.1+ and JetBrains GitHub Plugin. This vulnerability could lead to disclosure of access tokens to third-party sites [1].

Technical Details

The vulnerability, identified as **CVE-2024-37051** with a CVSS score of 9.3 [2], affects pull requests within the IntelliJ-based IDEs. Specifically, malicious content included in a pull request to a GitHub project, when handled by IntelliJ-based IDEs, could lead to exposure of access tokens to a third-party host.

Affected Products

The fixed versions are listed below. All previous versions are considered vulnerable [1].

- 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
- WebStorm: 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4

Recommendations and Mitigation

It is recommended to apply updates as soon as possible on affected products. Additionally, it is advised to revoke any GitHub tokens being used by JetBrains GitHub Plugin. The plugin can use OAuth integration or Personal Access Token (PAT). Follow the steps below to revoke access [1]:

- **OAuth Integration Settings**: Go to Applications [3] → Authorized OAuth Apps and revoke access for the **JetBrains IDE Integration** application.
- **Personal Access Token Settings**: Go to the Tokens [4] page and delete the token issued for the plugin. The default token name is **IntelliJ IDEA GitHub integration plugin**.

References

[1] https://blog.jetbrains.com/security/2024/06/updates-for-security-issue-affecting-intellij-based-ides-2023-1-and-github-plugin/

[2] https://nvd.nist.gov/vuln/detail/CVE-2024-37051

[3] https://github.com/settings/applications

[4] https://github.com/settings/tokens