مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

JetBrains Security Updates

Tracking #:432319235

Date:03-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed JetBrains has released security updates addressing multiple vulnerabilities affecting JetBrains Hub, YouTrack Server, GoLand, and Kotlin.

TECHNICAL DETAILS:

JetBrains has released security updates addressing multiple vulnerabilities affecting JetBrains Hub, YouTrack Server, GoLand, and Kotlin. The most critical vulnerability, CVE-2026-50242 (CVSS 10.0), allows an attacker with direct database access to bypass authentication and gain administrative privileges over JetBrains Hub and YouTrack Server instances. Additional vulnerabilities include a critical privilege escalation flaw (CVE-2026-56142), an account takeover vulnerability (CVE-2026-56141), and a remote code execution (RCE) vulnerability in GoLand (CVE-2026-53915). Multiple medium- and low-severity vulnerabilities affecting YouTrack and Kotlin have also been addressed. Although JetBrains has stated that no evidence of active exploitation or public proof-of-concept (PoC) is currently available, organizations operating self-managed JetBrains products should apply the latest security updates immediately.

Product	Description	Severity	Resolved In	CVE
Hub	Account takeover via predictable restore codes was possible. Reported by Ngoc Thuan (HUB-13105)	Critical	2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429	CVE-2026-56141
Hub	Privilege escalation by attaching authentication details to accounts was possible (HUB-13158)	Critical	2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429	CVE-2026-56142
Hub	Authentication bypass via direct database access leading to administrative access was possible. Reported by Tuan Anh Lai (HUB-13079)	Critical	2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429	CVE-2026-50242
YouTrack	Authentication bypass via direct database access leading to administrative access was possible. Reported by Ngoc Thuan (JT-96173)	Critical	2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429	CVE-2026-50242

GoLand	Remote code execution was possible via untrusted project configuration (GO-20428)	High	2026.1.3	CVE-2026-53915
Kotlin	Code execution was possible via unsafe deserialization in the build cache metadata. Reported by Sherry Zhou (KT-86604)	Medium	2.4.20	CVE-2026-53914
YouTrack	Improper access control allowed reading users' private data via the comment templates endpoint. Reported by 0xmoose (JT-96011)	Medium	2026.2.16593	CVE-2026-57921
YouTrack	Project settings disclosure via the MCP was possible. Reported by snifyak (JT-95932)	Low	2026.2.16593	CVE-2026-57922
YouTrack	Improper authorisation in the app configurations endpoint allowed modifying project settings. Reported by kalkii (JT-95931)	Medium	2026.2.16593	CVE-2026-57923
YouTrack	Default role configuration exposed excessive user profile details. Reported by 0xmoose (JT-95674)	Medium	2026.2.16593	CVE-2026-57924
YouTrack	Improper access control allowed reading saved queries and tags. Reported by Tushar Sharma (JT-95672)	Medium	2026.2.16593	CVE-2026-57925
YouTrack	The websandbox bridge was vulnerable to a prototype pollution attack (JT-96770)	Low	2026.2.16593	CVE-2026-57926

RECOMMENDATIONS:

Immediate Actions:

- Upgrade JetBrains Hub, YouTrack Server, GoLand, Kotlin to the latest fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.jetbrains.com/privacy-security/issues-fixed/