مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - JetBrains

Tracking #:432319343

Date:27-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that JetBrains has released security updates to address multiple vulnerabilities in GoLand, IntelliJ IDEA, PhpStorm, PyCharm, TeamCity, and WebStorm.

TECHNICAL DETAILS:

JetBrains has released security updates addressing multiple vulnerabilities across GoLand, IntelliJ IDEA, PhpStorm, PyCharm, TeamCity, and WebStorm.
The most severe issues, CVE-2026-64812 and CVE-2026-64813 (CVSS 10.0), affect IntelliJ IDEA Remote Development, allowing unauthorized input injection and configuration changes due to missing authentication and improper client-side enforcement. Additionally, TeamCity received fixes for two high-risk code execution vulnerabilities that could impact CI/CD environments.

Notable Vulnerabilities

CVE	CVSS	Description	Fixed Version(s)
CVE-2026-64812	10.0	Missing authentication enables unauthorized input injection during Remote Development sessions (CWE-306).	2026.2
CVE-2026-64813	10.0	Improper client-side enforcement allows unauthorized settings modification in Remote Development (CWE-602).	2026.2
CVE-2026-65907	9.1	Code execution through TeamCity Git VCS Roots (CWE-94).	2026.1.2, 2025.11.6
CVE-2026-65906	8.8	Kotlin DSL sandbox escape in TeamCity leading to code execution (CWE-94).	2026.1.2, 2025.11.6
CVE-2026-64814	8.6	Unauthorized file access in Remote Development (CWE-862).	2026.2
CVE-2026-65908	8.6	Untrusted component inclusion vulnerability (CWE-829).	2026.1.4, 2026.2
CVE-2026-64804	8.4	Untrusted component inclusion (CWE-829).	2026.2
CVE-2026-64805	8.4	Untrusted component inclusion (CWE-829).	2026.2

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, bypass Project Trust protections, modify Remote Development sessions, access sensitive files, and compromise TeamCity build servers. This could lead to theft of source code and credentials, disruption of CI/CD pipelines, software supply chain compromise, and unauthorized access to development environments.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by JetBrains.

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/