Fixed security issues

This page contains information about resolved security issues, including description, severity, assigned CVEs, and the product versions in which they were resolved.

Product

Select item

Fix version

Select item

Product	Description	Severity	Resolved In	CWE
Junie	Command execution was possible via a malicious project file. Reported by Aaron Portnoy/Mindgard (JUNIE-1108)	Medium	252.549.29	CWE-77

Product	Description	Severity	Resolved In	CWE
YouTrack	High privileged user can achieve RCE via sandbox bypass. Reported by Hacktron AI and Rahul Maini	High	2025.3.131383	CWE-1336
Datalore	Session hijacking was possible due to missing secure attribute for cookie settings. Reported by Antoni Tremblay (DL-16814)	Medium	2026.1	CWE-614
Hub	Possible on sign-in account mismatch with non-SSO auth and 2FA disabled. Reported by Guillaume Duval (HUB-12853)	Medium	2025.3.128064	CWE-290
TeamCity	Open redirect was possible in the React project creation flow (TW-97559)	Medium	2025.11.3	CWE-601
TeamCity	Missing authorization allowed project developers to add parameters to build configurations (TW-98760)	Medium	2025.11.3	CWE-862
TeamCity	Disabling versioned settings left a credentials config on disk (TW-98338)	Low	2025.11.3	CWE-459
YouTrack	Apps were able to send requests to the app	High	2025.3.121962	CWE-862

Product	Description	Severity	Resolved In	CWE
	permissions endpoint. Reported by Silas Porth (JT-94055)			
Hub	Authentication bypass allowing administrative actions was possible. Reported by "brbr0s" (HUB-12763)	Critical	2025.3.119807	CWE-306
PyCharm	A DOM-based XSS on Jupyter viewer page was possible. Reported by Yaniv Nizry (PY-85539)	High	2025.3.2	CWE-79
YouTrack	Access tokens could be exposed in Mailbox logs (JT-93573)	Medium	2025.3.119033	CWE-532
dotTrace	Local privilege escalation possible via race condition (DTRC-31841)	Medium	2025.2.5	CWE-367
ReSharper	Local privilege escalation possible via race condition (DTRC-31841)	Medium	2025.2.5	CWE-367
Rider	Local privilege escalation possible via race condition (DTRC-31841)	Medium	2025.2.5	CWE-367
IntelliJ IDEA	Missing confirmation allowed opening of untrusted remote projects over SSH (IJPL-196907)	Medium	2025.3	CWE-349
TeamCity	Maven embedder allowed loading extensions via	Low	2025.11	CWE-829

Product	Description	Severity	Resolved In	CWE
	project configuration (TW-95390)			
TeamCity	Stored XSS was possible on agentpushInstall page (TW-95022)	Low	2025.11	CWE-79
TeamCity	Port enumeration was possible via the Perforce connection test (TW-95764)	Low	2025.11	CWE-203
TeamCity	Reflected XSS was possible on VCS Root setup (TW-95741)	Medium	2025.11	CWE-79
TeamCity	A DOM-based XSS was possible on the OAuth connections tab (TW-95740)	Medium	2025.11	CWE-79
TeamCity	Excessive privileges were possible due to storing GitHub personal access token instead of an installation token (TW-97528)	Medium	2025.11.1	CWE-272
TeamCity	Reflected XSS was possible on the storage settings page (TW-96226)	Medium	2025.11.1	CWE-79
TeamCity	Improper repository URL validation could lead to local paths disclosure (TW-93129)	Low	2025.11.2	CWE-939

Product	Description	Severity	Resolved In	CWE
TeamCity	Improper access control could expose GitHub App token's metadata (TW-96318)	Low	2025.11	CWE-863
TeamCity	Stored XSS was possible via session attribute (TW-88600)	Medium	2025.11	CWE-79
TeamCity	Path traversal was possible via file upload (TW-96268)	Low	2025.11	CWE-22
YouTrack	A race condition allowed bypass of helpdesk Agent limit. Reported by "brbr0s" (JT-92337)	Low	2025.3.104432	CWE-362
Hub	A race condition allowed bypass of the user limit via invitations. Reported by "brbr0s" (HUB-12556)	Low	2025.3.104992	CWE-862
Hub	A race condition allowed bypass of the Agent-user limit. Reported by "brbr0s" (HUB-12560)	Low	2025.3.104432	CWE-362
Hub	Information disclosure was possible via the Users API (HUB-12279)	Medium	2025.3.104432	CWE-362
ReSharper	Missing signature verification in DPA Collector allows local privilege escalation (DPA-3467)	High	2025.2.4	CWE-347

Product	Description	Severity	Resolved In	CWE
Rider	Missing signature verification in DPA Collector allows local privilege escalation (DPA-3467)	High	2025.2.4	CWE-347
YouTrack	Information disclosure was possible via the feedback form (JT-91862)	Medium	2025.3.104432	CWE-862
YouTrack	Missing TLS certificate validation enabled data disclosure (JT-91555)	High	2025.3.104432	CWE-295
Junie	Code execution was possible due to improper command validation. Reported by Ari Marzouk "MaccariTA" (JUNIE-595)	High	252.284.50, 251.284.50, 243.284.50	CWE-77
TeamCity	Project isolation bypass was possible due to race condition (TW-94772)	Medium	2025.07.2	CWE-362
TeamCity	Path traversal was possible during project archive upload (TW-88604)	Medium	2025.07.2	CWE-23
TeamCity	Missing Git URL validation allowed credential leakage on Windows (TW-94701)	High	2025.07.2	CWE-183
IDE Services	Users without appropriate permissions could assign high-privileged role for themselves (IDES-9991)	High	2025.5.0.1086, 2025.4.2.2164	CWE-862

Product	Description	Severity	Resolved In	CWE
Junie	Information disclosure was possible via search_project function. Reported by Ari Marzouk "MaccariTA" (JUNIE-228)	Medium	252.284.50, 251.284.50, 243.284.50	CWE-356
IntelliJ IDEA	Credentials disclosure was possible via remote reference (IJPL-171671)	Medium	2025.2, 2025.1.2	CWE-319
IntelliJ IDEA	Improper access control allowed Code With Me guest to discover hidden files (IJPL-188779)	Medium	2025.2	CWE-863
IntelliJ IDEA	Unexpected plugin startup was possible due to automatic LSP server start (IJPL-183192)	Medium	2025.2, 2025.1.2	CWE-829
IntelliJ IDEA	HTML injection was possible via Remote Development feature. Reported by Marcin Bobryk (IJPL-181293)	Medium	2025.2	CWE-80
TeamCity	Privilege escalation was possible due to incorrect directory ownership (TW-94812)	High	2025.07.1	CWE-282
TeamCity	SMTP injection was possible allowing modification of email content. Reported by b1u3r and 1ue (TW-94836)	Medium	2025.07.1	CWE-77

Product	Description	Severity	Resolved In	CWE
TeamCity	AWS credentials were exposed in Docker script files (TW-92252)	Medium	2025.07.1	CWE-538
YouTrack	Stored XSS was possible via Mermaid diagram content. Reported by Chris Grieger (JT-90843)	High	2025.2.92387	CWE-79
TeamCity	A CSRF was possible in GitHub App connection flow (TW-93017)	Medium	2025.07	CWE-352
TeamCity	A CSRF was possible in external OAuth login integration (TW-93013)	Low	2025.07	CWE-352
TeamCity	Privilege escalation was possible due to incorrect directory permissions. Reported by CrisprXiang and Hao Huang from FDU (TW-92560)	High	2025.07	CWE-276
TeamCity	Path traversal was possible via plugin unpacking on Windows. Reported by Thomas Siegbert (TW-93925)	High	2025.07	CWE-23
TeamCity	Improper access control allowed disclosure of build settings via snapshot dependencies (TW-39209)	Medium	2025.07	CWE-863
TeamCity	Improper access control allowed disclosure of	Medium	2025.07	CWE-863

Product	Description	Severity	Resolved In	CWE
	build settings via VCS configuration (TW-39192)			
TeamCity	Reflected XSS was possible on the agentpushPreset page (TW-84016)	Medium	2025.07	CWE-79
TeamCity	Password reset and email verification tokens were using weak hashing algorithms (TW-85813)	Medium	2025.07	CWE-328
TeamCity	A CSRF was possible on GraphQL endpoint (TW-93015)	Medium	2025.07	CWE-352
TeamCity	User credentials were stored in plain text in memory snapshots (TW-78814)	Medium	2025.07	CWE-312
TeamCity	Password exposure was possible via command line in the "hg pull" command (TW-34488)	Medium	2025.07	CWE-312
YouTrack	Improper iframe configuration in widget sandbox allows popups to bypass security restrictions. Reported by Sebastian Schmitt (JT-90347)	Medium	2025.2.86935, 2025.2.87167, 2025.3.87341, 2025.3.87344	CWE-1021
YouTrack	Email spoofing via an administrative API was possible (JT-90065)	High	2025.2.86069, 2024.3.85077, 2025.1.86199	CWE-862

Product	Description	Severity	Resolved In	CWE
TeamCity	A DOM-based XSS at the Performance Monitor page was possible (TW-93018)	Medium	2025.03.3	CWE-79
TeamCity	Reflected XSS on the favoriteIcon page was possible (TW-92954)	Medium	2025.03.3	CWE-79
TeamCity	Reflected XSS on diskUsageBuildsStats page was possible (TW-92952)	Medium	2025.03.3	CWE-79
TeamCity	Usernames were exposed to the users without proper permissions (TW-93038)	Medium	2025.03.3	CWE-862
TeamCity	Reflected XSS in the NPM Registry integration was possible. Reported by Alex Williams from Converge Technology Solutions (TW-93108)	Medium	2025.03.3	CWE-79
TeamCity	Stored XSS via GitHub Checks Webhook was possible. Reported by Alex Williams from Converge Technology Solutions (TW-93107)	Medium	2025.03.2	CWE-79
TeamCity	Stored XSS via YouTrack integration was possible. Reported by Alex Williams from Converge	Medium	2025.03.2	CWE-79

Product	Description	Severity	Resolved In	CWE
	Technology Solutions (TW-93109)			
TeamCity	Stored XSS via Jira integration was possible. Reported by Alex Williams from Converge Technology Solutions (TW-93110)	Medium	2025.03.2	CWE-79
TeamCity	Open redirect was possible on editing VCS Root page (TW-93019)	Medium	2025.03.2	CWE-601
YouTrack	Deletion of issues was possible due to missing permission checks in API. Reported by Matthias Schorsch (JT-89365)	High	2025.1.76253	CWE-306
YouTrack	Restricted attachments could become visible after issue cloning (JT-89030)	Medium	2025.1.74704	CWE-306
Rider	Custom archive unpacker allowed arbitrary file overwrite during remote debug session (RIDER-121315)	Medium	2025.1.2	CWE-23
TeamCity	Base64-encoded credentials could be exposed in build logs (TW-92598)	Medium	2025.03.1	CWE-532
TeamCity	Improper path validation in loggingPreset	Medium	2025.03.1	CWE-23

Product	Description	Severity	Resolved In	CWE
	parameter was possible (TW-92692)			
TeamCity	Stored XSS was possible on Data Directory tab. Reported by Grigory Dorodnov of Trend Micro (TW-92511)	Low	2025.03.1	CWE-79
RubyMine	Remote Interpreter overwrote ports to listen on all interfaces. Reported by Rainer Killinger (RUBY-33848)	High	2025.1	CWE-1188
Toolbox App	Host key verification was missing in SSH plugin (TBX-13080)	Medium	2.6	CWE-297
Toolbox App	Command injection in SSH plugin was possible (TBX-13929)	High	2.6	CWE-77
Toolbox App	Unencrypted credential transmission during SSH authentication was possible (TBX-11543)	Medium	2.6	CWE-319
Toolbox App	The SSH plugin established connections without sufficient user confirmation (TBX-13079)	Medium	2.6	CWE-304
IntelliJ IDEA	Source code could be logged in the idea.log file. Reported by scscid (IJPL-162443)	Low	2024.3, 2024.2.4	CWE-532

Product	Description	Severity	Resolved In	CWE
TeamCity	Base64 encoded password could be exposed in build log (TW-91934)	Medium	2025.03	CWE-532
TeamCity	Stored XSS was possible on Cloud Profiles page (TW-92117)	Medium	2025.03	CWE-79
TeamCity	Exception could lead to credential leakage on Cloud Profiles page (TW-89110)	Low	2025.03	CWE-209
GoLand	An XXE during debugging was possible. Reported by Thanh Nguyen (GO-18010)	Medium	2025.1	CWE-611
JetBrains Runtime	Arbitrary dynamic library execution due to insecure macOS flags was possible. Reported by Waleed Barakat of TikTok US Data Security (JBR-8138)	Medium	21.0.6b872.80	CWE-426
Ktor	HTTP Request Smuggling was possible. Reported by Jeppe Bonde Weikop (KTOR-8015)	Medium	3.1.1	CWE-444
TeamCity	Several DOM-based XSS were possible on the Code Inspection Report tab (TW-87505)	Medium	2024.12.2	CWE-79

Product	Description	Severity	Resolved In	CWE
TeamCity	Improper Kubernetes connection settings could expose sensitive resources (TW-91106)	High	2024.12.2	CWE-522
dotTrace	Local Privilege Escalation via the ETW Host Service was possible (DTRC-31503)	High	2024.3.4, 2024.2.8, 2024.1.7	CWE-114
ETW Host Service	Local Privilege Escalation via the ETW Host Service was possible (DTRC-31503)	High	16.43	CWE-114
ReSharper	Local Privilege Escalation via the ETW Host Service was possible (DTRC-31503)	High	2024.3.4, 2024.2.8, 2024.1.7	CWE-114
Rider	Local Privilege Escalation via the ETW Host Service was possible (DTRC-31503)	High	2024.3.4, 2024.2.8, 2024.1.7	CWE-114
Hub	Privilege escalation was possible via LDAP authentication mapping. Reported by Pavel Supruniuk (HUB-12012)	Medium	2024.3.55417	CWE-288
TeamCity	Reflected XSS was possible on the Vault Connection page (TW-91124)	Medium	2024.12.1	CWE-79
TeamCity	Improper access control allowed to see Projects’	Medium	2024.12.1	CWE-863

Product	Description	Severity	Resolved In	CWE
	names in the agent pool (TW-52375, TW-91367)			
TeamCity	Decryption of connection secrets without proper permissions was possible via Test Connection endpoint (TW-91164)	Medium	2024.12.1	CWE-862
YouTrack	Permanent token could be exposed in logs when token is malformed and cannot be parsed. Reported by Dmitriy Titarenko (JT-86763)	Medium	2024.3.55417	CWE-532
YouTrack	Account takeover was possible via spoofed email and Helpdesk integration (JT-85444)	High	2024.3.55417	CWE-290
TeamCity	Improper access control allowed viewing details of unauthorized agents (TW-85841)	Medium	2024.12	CWE-863
TeamCity	Improper access control allowed unauthorized users to modify build logs (TW-90726)	Medium	2024.12	CWE-862
TeamCity	Build credentials allowed unauthorized viewing of projects (TW-24904)	Medium	2024.12	CWE-863
TeamCity	Access tokens were not revoked after removing user roles (TW-76910)	Medium	2024.12	CWE-613

Product	Description	Severity	Resolved In	CWE
TeamCity	Stored XSS was possible via image name on the agent details page (TW-89485)	Medium	2024.12	CWE-79
TeamCity	Backup file exposed user credentials and session cookies. Reported by Thomas Siegbert (TW-89719)	Medium	2024.12	CWE-212
TeamCity	Password field value were accessible to users with view settings permission (TW-49870)	Medium	2024.12	CWE-522
TeamCity	Missing Content-Type header in RemoteBuildLogController response could lead to XSS (TW-80940)	Medium	2024.12	CWE-79
TeamCity	Insecure XMLParser configuration could lead to potential XXE attack (TW-86582)	Medium	2024.12	CWE-611
YouTrack	Unauthenticated database backup download was possible via vulnerable query parameter (JT-85385)	Low	2024.3.51866	CWE-862
YouTrack	System takeover was possible through path traversal in plugin sandbox (JT-85298)	High	2024.3.51866	CWE-23

Product	Description	Severity	Resolved In	CWE
YouTrack	Improper access control allowed listing of project names during app import without authentication. Reported by Tom Gionfriddo (JT-85830)	Low	2024.3.51866	CWE-862
YouTrack	Multiple merge functions were vulnerable to prototype pollution attack (JT-85614)	Medium	2024.3.52635	CWE-1321
YouTrack	Potential ReDoS was possible due to vulnerable RegExp in Ruby syntax detector (JT-85443)	Medium	2024.3.52635	CWE-1333
YouTrack	Potential spoofing attack was possible via lack of Punycode encoding (JT-85607)	Low	2024.3.52635	CWE-173
WebStorm	Code execution in Untrusted Project mode was possible via type definitions installer script. Reported by Ramast Magdy (WEB-69576)	Medium	2024.3	CWE-349
Hub	Improper access control allowed users to generate permanent tokens for unauthorized services (HUB-11932)	Medium	2024.3.47707	CWE-862

Product	Description	Severity	Resolved In	CWE
YouTrack	Potential ReDoS exploit was possible via email header parsing in Helpdesk functionality (JT-85386)	Medium	2024.3.47707	CWE-1333
YouTrack	Reflected XSS was possible in Widget API (JT-85387)	Medium	2024.3.47707	CWE-79
YouTrack	Stored XSS was possible via vendor URL in App manifest (JT-85389)	Medium	2024.3.47707	CWE-79
YouTrack	Stored XSS was possible via Angular template injection in Hub settings (JT-85384)	Medium	2024.3.47707	CWE-79
YouTrack	Stored XSS was possible via sprint value on agile boards page (JT-85299)	Medium	2024.3.47707	CWE-79
YouTrack	Reflected XSS due to insecure link sanitization was possible (JT-85383)	Medium	2024.3.47707	CWE-79
YouTrack	Multiple XSS were possible due to insecure markdown parsing and custom rendering rule (JT-85295)	Medium	2024.3.47707	CWE-79
YouTrack	Improper HTML sanitization could lead to XSS attack via comment tag (JT-85296)	Medium	2024.3.47707	CWE-79

Product	Description	Severity	Resolved In	CWE
YouTrack	Stored XSS was possible due to improper HTML sanitization in markdown elements (JT-85297)	Medium	2024.3.47707	CWE-79
Ktor	Improper caching in HttpCache Plugin could lead to response information disclosure. Reported by Nils Barlaug (KTOR-7483)	Medium	2.3.13	CWE-524
YouTrack	Insecure plugin iframe allowed arbitrary JavaScript execution and unauthorized API requests (JT-85294)	High	2024.3.47197	CWE-940
YouTrack	Improper access control allowed users with project update permission to delete applications via API	Medium	2024.3.46677	CWE-862
TeamCity	Password could be exposed via Sonar runner REST API (TW-64557)	Medium	2024.07.3	CWE-522
TeamCity	Path traversal leading to information disclosure was possible via server backups. Reported by Thomas Siegbert (TW-89721)	Medium	2024.07.3	CWE-23
TeamCity	Path traversal allowed backup file write to arbitrary location.	Medium	2024.07.3	CWE-23

Product	Description	Severity	Resolved In	CWE
	Reported by Thomas Siegbert (TW-89723)			
TeamCity	Stored XSS was possible in Backup configuration settings. Reported by Thomas Siegbert (TW-89700)	Low	2024.07.3	CWE-79
TeamCity	Stored XSS was possible via server global settings (TW-88983)	Low	2024.07.3	CWE-79
YouTrack	User without appropriate permissions could restore workflows attached to a project (JT-82431)	Medium	2024.3.44799	CWE-863
YouTrack	Access to global app config data without appropriate permissions was possible (JT-81376)	Medium	2024.3.44799	CWE-863
YouTrack	Token could be revealed on Imports page (JT-82142)	Medium	2024.3.44799	CWE-522
IntelliJ IDEA	HTML injection via the project name was possible (IJPL-8358)	Low	2024.1	CWE-79
TeamCity	Possible privilege escalation due to incorrect directory permissions. Reported by Crispr Xiang from TianShu Dubhe Team (TW-87656)	High	2024.07.1	CWE-276

Product	Description	Severity	Resolved In	CWE
TeamCity	Multiple stored XSS was possible on Clouds page (TW-85512)	Medium	2024.07.1	CWE-79
TeamCity	Self XSS was possible in the HashiCorp Vault plugin (TW-84492)	Low	2024.07.1	CWE-79
TeamCity	Reflected XSS was possible on the agentPushPreset page (TW-84016)	Low	2024.07.1	CWE-79
TeamCity	Reflected XSS was possible in the AWS Core plugin (TW-86958)	Medium	2024.07.1	CWE-79
TeamCity	Parameters of the "password" type could leak into the build log in some specific cases (TW-67957)	Medium	2024.07	CWE-532
TeamCity	Stored XSS was possible on the Code Inspection tab (TW-83483)	Medium	2024.07	CWE-79
TeamCity	Stored XSS was possible on Show Connection page (TW-86935)	Low	2024.07	CWE-79
TeamCity	Access tokens could continue working after deletion or expiration (TW-76857)	High	2024.07	CWE-613
TeamCity	Comparison of authorization tokens took	Low	2024.07	CWE-208

Product	Description	Severity	Resolved In	CWE
	non-constant time (TW-85815)			
TeamCity	An OAuth code for JetBrains Space could be stolen via Space Application connection (TW-84124)	Low	2024.07	CWE-303
TeamCity	Private key could be exposed via testing GitHub App Connection (TW-88255)	Medium	2024.03.3	CWE-522
TeamCity	Application token could be exposed in EC2 Cloud Profile settings (TW-88399)	Medium	2024.03.3	CWE-522
Hub	Stored XSS via project description was possible. Reported by Krzysztof Kamiński (HUB-11601)	Low	2024.2.34646	CWE-79
YouTrack	The Guest User Account was enabled for attaching files to articles (JT-81902)	Medium	2024.2.34646	CWE-862
YouTrack	User access token was sent to the third-party site. Reported by Sergey Zotov (JT-81798)	Medium	2024.2.34646	CWE-522
YouTrack	User without appropriate permissions could enable the auto-attach option for workflows (JT-81214)	Medium	2024.2.34646	CWE-862

Product	Description	Severity	Resolved In	CWE
Aqua	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2024.1.2	CWE-522
CLion	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2	CWE-522
DataGrip	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4	CWE-522
DataSpell	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1	CWE-522
GoLand	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3	CWE-522
IntelliJ IDEA	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3	CWE-522
MPS	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.2.1, 2023.3.1, 2024.1 EAP2	CWE-522

Product	Description	Severity	Resolved In	CWE
PhpStorm	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3	CWE-522
PyCharm	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2	CWE-522
Rider	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3	CWE-522
RubyMine	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4	CWE-522
RustRover	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2024.1.1	CWE-522
WebStorm	GitHub access token could be exposed to third-party sites (IJPL-155883)	Critical	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	CWE-522
TeamCity	Path traversal allowing to read files from server was possible (TW-87898)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5, 2024.03.2	CWE-23

Product	Description	Severity	Resolved In	CWE
TeamCity	Several Stored XSS in code inspection reports were possible (TW-83495)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79
TeamCity	Improper access control in Pull Requests and Commit status publisher build features was possible (TW-84931)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-863
TeamCity	A third-party agent could impersonate a cloud agent (TW-87450)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5, 2024.03.2	CWE-863
TeamCity	An XSS could be executed via certain report grouping and filtering operations (TW-83893)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79
TeamCity	Stored XSS via third-party reports was possible (TW-83270)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79
TeamCity	Reflected XSS via OAuth provider configuration was possible (TW-83485)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79
TeamCity	Stored XSS via issue tracker integration was possible (TW-83149)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79

Product	Description	Severity	Resolved In	CWE
TeamCity	Stored XSS via OAuth connection settings was possible (TW-83658)	Medium	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-79
TeamCity	Stored XSS in Commit status publisher was possible (TW-84958)	Medium	2023.05.6, 2023.11.5	CWE-79
TeamCity	Reflected XSS on the subscriptions page was possible (TW-83892)	Medium	2023.05.6	CWE-79
TeamCity	Several stored XSS in untrusted builds settings were possible (TW-87421)	Medium	2024.03.2	CWE-79
TeamCity	Stored XSS via build step settings was possible (TW-87381)	Medium	2024.03.2	CWE-79
TeamCity	Technical information regarding TeamCity server could be exposed (TW-87468)	Medium	2024.03.2	CWE-209
TeamCity	Users could perform actions that should not be available to them based on their permissions (TW-83710)	Medium	2024.03.2	CWE-863
TeamCity	Certain TeamCity API endpoints did not check user permissions (TW-83647)	Medium	2024.03.2	CWE-863

Product	Description	Severity	Resolved In	CWE
TeamCity	Server was susceptible to DoS attacks with incorrect auth tokens (TW-87071)	Medium	2024.03.2	CWE-770
TeamCity	Authentication bypass was possible in specific edge cases even when the security patch plugin is intstalled (TW-86860)	High	2022.04.7, 2022.10.6, 2023.05.6, 2023.11.5	CWE-288
TeamCity	Several Stored XSS in the available updates page were possible (TW-87050)	Low	2024.03.1	CWE-79
TeamCity	Commit status publisher didn't check project scope of the GitHub App token (TW-86523)	Medium	2024.03.1	CWE-280
TeamCity	Stored XSS during restore from backup was possible (TW-82309)	Medium	2023.11	CWE-79
YouTrack	The SMTPS protocol communication lacked proper certificate hostname validation. Reported by Yusuke Yamamoto (JT-80708)	Medium	2024.1.29548	CWE-295
TeamCity	Authenticated users without administrative permissions could register other users when self-registration was disabled (TW-87046)	Medium	2024.03	CWE-863

Product	Description	Severity	Resolved In	CWE
TeamCity	Open redirect was possible on the login page (TW-87062)	Medium	2024.03	CWE-601
TeamCity	2FA could be bypassed by providing a special URL parameter (TW-86989)	High	2024.03	CWE-1288
TeamCity	Reflected XSS was possible via Space connection configuration. Reported by Linh Dinh (TW-86832)	Medium	2024.03	CWE-79
TeamCity	XSS was possible via Agent Distribution settings. Reported by Alex Williams from Trend Micro (TW-86535)	Medium	2024.03	CWE-79
TeamCity	XXE was possible in the Maven build steps detector (TW-86300)	Medium	2024.03	CWE-611
TeamCity	Server administrators could remove arbitrary files from the server by installing tools (TW-86039)	Medium	2024.03	CWE-1288
TeamCity	Users with access to the agent machine might obtain permissions of the user running the agent process (TW-83048)	Medium	2023.11	CWE-749
YouTrack	Creation comments on behalf of an arbitrary user	Medium	2024.1.25893	CWE-290

Product	Description	Severity	Resolved In	CWE
	in HelpDesk was possible (JT-79678, JT-79719)			
YouTrack	User without appropriate permissions could restore issues and articles (JT-79924)	Medium	2024.1.25893	CWE-863
YouTrack	Attaching/detaching workflow to a project was possible without project admin permissions (JT-79758)	Medium	2024.1.25893	CWE-862
TeamCity	Custom build parameters of the "password" type could be disclosed (TW-86403)	Medium	2023.11.4	CWE-201
TeamCity	Presigned URL generation requests in S3 Artifact Storage plugin were authorized improperly (TW-85562)	Medium	2023.11.4	CWE-863
TeamCity	Authentication bypass allowing to perform admin actions was possible. Reported by Rapid7 team (TW-86500)	Critical	2023.11.4	CWE-288
TeamCity	Path traversal allowing to perform limited admin actions was possible. Reported by Rapid7 team (TW-86502)	High	2023.11.4	CWE-23

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	Path traversal was possible when unpacking archives (IDEA-339542)	Low	2023.3.3	CWE-23
IntelliJ IDEA	A plugin for JetBrains Space was able to send an authentication token to an inappropriate URL (IDEA-337274)	Medium	2023.3.3	CWE-20
Rider	Logging of environment variables containing secret values was possible (RIDER-103340)	Low	2023.3.3	CWE-532
TeamCity	Path traversal allowed reading data within JAR archives. Reported by Sndav Bai and Crispr Xiang from TianShu Dubhe Team (TW-86017)	Medium	2023.11.3	CWE-23
TeamCity	Authentication bypass leading to RCE was possible. Reported by Sndav Bai and Crispr Xiang from TianShu Dubhe Team (TW-86005)	Critical	2023.11.3	CWE-288
Toolbox App	A DoS attack was possible via a malicious SVG image (TBX-9216)	Medium	2.2	CWE-400
TeamCity	Access control at the S3 Artifact Storage plugin endpoint was missed (TW-85499)	Medium	2023.11.2	CWE-285

Product	Description	Severity	Resolved In	CWE
TeamCity	Stored XSS via agent distribution was possible (TW-85880)	Medium	2023.11.2	CWE-79
TeamCity	Limited directory traversal was possible in the Kotlin DSL documentation (TW-85585)	Medium	2023.11.2	CWE-23
YouTrack	Stored XSS via markdown was possible. Reported by Sergei Zotov (JT-78995)	Medium	2023.3.22666	CWE-79
IntelliJ IDEA	Code execution was possible in Untrusted Project mode via a malicious plugin repository specified in the project configuration (IDEA-320814)	Medium	2023.3.2	CWE-349
TeamCity	A CSRF on login was possible (TW-84796)	Medium	2023.11.1	CWE-352
YouTrack	Authorization check for inline comments inside thread replies was missed (JT-78444)	Medium	2023.3.22268	CWE-285
Ktor	Default configuration of ContentNegotiation with XML format was vulnerable to XXE. Reported by Ulf Karlsson (KTOR-6286, Pull Request)	High	2.3.5	CWE-611

Product	Description	Severity	Resolved In	CWE
Ktor	Server certificates were not verified (KTOR-6229, Pull Request)	Medium	2.3.5	CWE-295
TeamCity	Authentication bypass leading to RCE on TeamCity Server was possible. Reported by Stefan Schiller from Sonar (TW-83545)	Critical	2023.05.4	CWE-288
TeamCity	Stored XSS was possible during nodes configuration (TW-83216)	Low	2023.05.4	CWE-79
TeamCity	Stored XSS was possible during Cloud Profiles configuration (TW-82867, TW-82475)	Medium	2023.05.3	CWE-79
TeamCity	Reflected XSS was possible during copying Build Step (TW-82869)	Medium	2023.05.3	CWE-79
TeamCity	Reflected XSS was possible during user registration (TW-82876)	Low	2023.05.3	CWE-79
IntelliJ IDEA	Plugin for Space was requesting excessive permissions (IDEA-321747)	Medium	2023.2	CWE-250
TeamCity	A token with limited permissions could be used to gain full account access (TW-82485)	Medium	2023.05.2	CWE-266

Product	Description	Severity	Resolved In	CWE
TeamCity	A ReDoS attack was possible via integration with issue trackers (TW-82283)	Medium	2023.05.2	CWE-1333
TeamCity	Reflected XSS via GitHub integration was possible (TW-82472)	Medium	2023.05.2	CWE-79
IntelliJ IDEA	License dialog could be suppressed in certain cases. Reported by Bilawal Imdad (IDEA-324171)	Low	2023.1.4	CWE-754
TeamCity	Stored XSS when using a custom theme was possible (TW-82270)	Medium	2023.05.1	CWE-79
TeamCity	Parameters of the "password" type could be shown in the UI in certain composite build configurations (TW-82022)	Medium	2023.05.1	CWE-200
TeamCity	Stored XSS while running custom builds was possible (TW-81723)	Medium	2023.05.1	CWE-79
TeamCity	Build chain parameters of the "password" type could be written to the agent log (TW-81846)	Medium	2023.05.1	CWE-532

Product	Description	Severity	Resolved In	CWE
TeamCity	Stored XSS while viewing the build log was possible (TW-81777)	Medium	2023.05.1	CWE-79
TeamCity	Reflected XSS via the Referer header was possible during artifact downloads (TW-80993)	Medium	2023.05.1	CWE-79
TeamCity	Build parameters of the "password" type could be written to the agent log (TW-80002)	Medium	2023.05.1	CWE-532
YouTrack	Captcha was not properly validated for Helpdesk forms (JT-75029)	Medium	2023.1.16597	CWE-799
YouTrack	A DoS attack was possible via Helpdesk forms (JT-75136)	High	2023.1.10518	CWE-400
YouTrack	Stored XSS in a Markdown-rendering engine was possible (JT-75230)	Medium	2023.1.10518	CWE-79
Ktor	Headers containing authentication data could be added to the exception's message (KTOR-5900, Pull Request)	Low	2.3.1	CWE-209
TeamCity	Bypass of permission checks allowing to perform admin actions	Critical	2023.05, 2022.10.4	CWE-863

Product	Description	Severity	Resolved In	CWE
	was possible. Reported by Isaac Peka (TW-81566)			
TeamCity	Improper permission checks allowed users without appropriate permissions to edit Build Configuration settings via REST API. Reported by Olof Lindberg (TW-80538)	Medium	2023.05, 2022.10.4	CWE-285
TeamCity	Stored XSS in the Commit Status Publisher window was possible (TW-80262)	Medium	2023.05, 2022.10.4	CWE-79
TeamCity	Stored XSS in the Show Connection page was possible (TW-81182)	Medium	2023.05	CWE-79
TeamCity	Possible XSS in the Plugin Vendor URL was possible (TW-80378)	Medium	2023.05	CWE-79
TeamCity	Parameters of the "password" type from build dependencies could be logged in some cases (TW-81338)	Medium	2023.05	CWE-532
TeamCity	Open redirect during oAuth configuration was possible (TW-79888)	Medium	2023.05	CWE-601
TeamCity	Stored XSS in the NuGet feed page was possible (TW-81031)	Medium	2023.05	CWE-79

Product	Description	Severity	Resolved In	CWE
TeamCity	Reflected XSS in the Subscriptions page was possible (TW-80881)	Medium	2023.05	CWE-79
TeamCity	A specific endpoint was vulnerable to brute force attacks (TW-80842)	Medium	2023.05, 2022.10.4	CWE-749
TeamCity	Authentication checks were missing – 2FA was not checked for some sensitive account actions (TW-73544)	Medium	2023.05	CWE-308
TeamCity	Stored XSS in GitLab Connection page was possible (TW-80174)	Medium	2023.05, 2022.10.4	CWE-79
Toolbox App	A DYLIB injection on macOS was possible. Reported by Dimitrie-Toma Furdui (TBX-9047)	Medium	1.28	CWE-691
Hub	SSRF protection in Auth Module integration was missing (HUB-11380)	Medium	2023.1.15725	CWE-918
Ktor	Path traversal in the `resolveResource` method was possible. Reported by Vasco Franco (KTOR-5733, Pull Request)	High	2.3.0	CWE-35
PhpStorm	Source code could be logged in the local idea.log file (WI-71063)	Low	2023.1	CWE-532

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	File content could be disclosed via an external stylesheet path in Markdown preview (IDEA-297583)	Medium	2023.1	CWE-200
IntelliJ IDEA	In some cases, Gradle and Maven projects could be imported without the “Trust Project” confirmation (IDEA-262839)	Medium	2023.1	CWE-345
IntelliJ IDEA	The bundled version of Chromium wasn't sandboxed (IDEA-284121)	Medium	2023.1	CWE-1188
IntelliJ IDEA	The NTLM hash could leak through an API method used in the IntelliJ IDEA built-in web server (IDEA-303249)	Medium	2023.1	CWE-522
Hub	Reflected XSS in dashboards was possible (HUB-11421)	Medium	2022.3.15573, 2022.2.15572, 2022.1.15583	CWE-79
TeamCity	Stored XSS in Perforce connection settings was possible (TW-79891)	Medium	2022.10.3	CWE-79
TeamCity	Stored XSS on “Pending changes” and “Changes” tabs was possible (TW-80199)	Medium	2022.10.3	CWE-79
TeamCity	Stored XSS on the SSH keys page was possible	Medium	2022.10.3	CWE-79

Product	Description	Severity	Resolved In	CWE
	(TW-80097)			
JetBrains Marketplace	There was a stored XSS vulnerability in the list of suggested plugins (MP-4822)	Medium	Not applicable	CWE-79
JetBrains Marketplace	Throttling was not in place for comment creation. Reported by Keroles Magdy (MP-4857)	Low	Not applicable	CWE-770
JetBrains Website	SSRF leading to AWS metadata disclosure was possible. Reported by Peter Af Geijerstam (JS-17660)	Medium	Not applicable	CWE-918
JetBrains Website	Server version and stack trace were disclosed to unauthorized users (JS-16718)	Low	Not applicable	CWE-209
JetBrains Website	It was possible to launch cookie bomb attacks, leading to DoS. Reported by Multansingh Medtiya (JS-17550)	Medium	Not applicable	CWE-703
JetBrains Website	There was a reflected XSS vulnerability in the Space instance registration process. Reported by Rahul Karki (SPACE-17966)	Medium	Not applicable	CWE-79
Space	Throttling was not in place for a password reset.	Low	Not applicable	CWE-770

Product	Description	Severity	Resolved In	CWE
	Reported by Hasan Khan (SPACE-17349)			
TeamCity	JVMTI was enabled by default on agents. Reported by Hj Chai (TW-78552)	Medium	2022.10.2	CWE-1188
TeamCity	There was an XSS vulnerability in the user creation process (TW-78783)	Medium	2022.10.2	CWE-79
TeamCity	There was an XSS vulnerability in the group creation process (TW-78786)	Medium	2022.10.2	CWE-79
JetBrains Marketplace	Stored XSS in the list of plugin ideas (MP-4824)	Medium	Not applicable	CWE-79
JetBrains Website	Reflected XSS in JetBrains Blog (JS-16355)	Medium	Not applicable	CWE-79
IntelliJ IDEA	The "Validate JSP File" action used the HTTP protocol to download required JAR files (IDEA-305732)	Medium	2022.3.1	CWE-319
IntelliJ IDEA	Code Templates were vulnerable to SSTI attacks. Reported by Krypton (IDEA-306345)	Medium	2022.3.1	CWE-1336
Space	The second authentication factor wasn't checked during the password	Medium	Not applicable	CWE-304

Product	Description	Severity	Resolved In	CWE
	reset. Reported by Bharat (SPACE-15087)			
IntelliJ IDEA	A buffer overflow in the fsnotifier daemon on macOS was possible (IDEA-302494)	Medium	2022.2.4	CWE-120
IntelliJ IDEA	The built-in web server leaked information about open projects (IDEA-297741)	Medium	2022.3	CWE-200
IntelliJ IDEA	The built-in web server allowed an arbitrary file to be read by exploiting a path traversal vulnerability (IDEA-304713)	Medium	2022.3	CWE-35
IntelliJ IDEA	An XXE attack leading to SSRF via requests to custom plugin repositories was possible (IDEA-302855)	Low	2022.3	CWE-611
IntelliJ IDEA	A DYLIB injection on macOS was possible. Independently reported by Anthony Viriya and Kang Ali (IDEA-298179)	Medium	2022.3	CWE-691
JetBrains Gateway	A client could connect without a valid token if the host consented (GTW-1786)	High	2022.3	CWE-287
Space	Profiles were improperly added to random projects,	Medium	Not applicable	CWE-668

Product	Description	Severity	Resolved In	CWE
	including restricted ones			
TeamCity	A custom STS endpoint allowed internal port scanning (TW-78415)	Medium	2022.10.1	CWE-918
TeamCity	Connecting to AWS using the "Default Credential Provider Chain" allowed TeamCity project administrators to access AWS resources normally limited to TeamCity system administrators (TW-78416)	Medium	2022.10.1	CWE-453
Hub	Throttling was missed when sending emails to a particular email address. Reported by Keroles Magdy (HUB-11260)	Low	2022.3.15181	CWE-770
TeamCity Cloud	EBS storage objects were not encrypted (TCC-175)	Low	Not applicable	CWE-311
TeamCity Cloud	Passwords for agent user accounts built from the same image were not randomized (TCC-188)	Medium	Not applicable	CWE-331
TeamCity	Excessive access permissions for secure token health items (TW-73518)	Low	2022.10	CWE-284
TeamCity	Project Viewer could see scrambled secure values	Medium	2022.10	CWE-538

Product	Description	Severity	Resolved In	CWE
	in the MetaRunner settings (TW-76796)			
TeamCity	Password parameters could be exposed in the build log if they contained special characters (TW-77048)	Medium	2022.10	CWE-532
TeamCity	No audit items were added upon editing a user's settings (TW-75537)	Low	2022.10	CWE-223
JetBrains Account	Throttling was missed on some pages. Reported by Manthan Mahale (JPF-13346)	Low	2022.09	CWE-770
TeamCity	Environmental variables of "password" type could be logged when using custom Perforce executable. Reported by Pierre Hosteins and Yvan Serykh (TW-77474)	Medium	2022.04.4	CWE-532
JetBrains Website	Open redirect on jetbrains.com.cn. Reported by Koutrouss Naddara (JS-17099)	Medium	Not applicable	CWE-601
IntelliJ IDEA	The installer was vulnerable to EXE search order hijacking. Reported by Dmitry Zemlyakov (IDEA-295424)	High	2022.2.2	CWE-427

Product	Description	Severity	Resolved In	CWE
JetBrains Website	The JetBrains blog was vulnerable to CSS injection (JS-16353)	Low	Not applicable	CWE-79
Ktor	Ktor was vulnerable to the Reflect File Download attack. Reported by Motoyasu Saburi (KTOR-4669, Pull Request)	Medium	2.1.0	CWE-184
Ktor	The wrong authentication provider could be selected in some cases. Reported by Andrew Bryan (KTOR-4618, Pull Request)	Medium	2.1.0	CWE-287
TeamCity	The private SSH key could be written to the server log in some cases (TW-76758)	Low	2022.04.3	CWE-532
Rider	*Trust and Open Project* dialog bypass, leading to local code execution (RIDER-74325, RIDER-74328)	Medium	2022.2	CWE-94
IntelliJ IDEA	Local code execution was possible via a Vagrant executable (IDEA-288325)	Low	2022.2	CWE-94

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	Missing email address validation in the "Git User Name Is Not Defined" dialog. Reported by Carolos Foscolos (IDEA-291960)	Low	2022.2	CWE-20
TeamCity	The private SSH key could be written to the build log in some cases (TW-76651)	Medium	2022.04.2	CWE-532
TeamCity	Build parameter injection was possible. Reported by Micky Sung (TW-76356)	Medium	2022.04.2	CWE-88
Hub	Insufficient access control allowed the hijacking of untrusted services in Hub. Reported by Yurii Sanin (HUB-10771)	Low	2022.2.14799	CWE-284
JetBrains Website	Potential XSS via Origin header. Reported by Nidhin Sabu (JPF-13063)	Low	Not applicable	CWE-79
Ktor	SHA1 implementation in Ktor Native was returning the same value (KTOR-4217, Pull Request)	High	2.0.1	CWE-342
TeamCity	Reflected XSS on the Build Chain Status page (TW-75231)	Medium	2022.04	CWE-79
TeamCity	Possible leak of secrets in TeamCity agent logs (TW-74263, TW-68807)	Medium	2022.04	CWE-532

Product	Description	Severity	Resolved In	CWE
TeamCity	Potential XSS via Referrer header (TW-75605)	Low	2022.04	CWE-79
Hub	Stored XSS via project icon. Reported by Julian Muñoz (HUB-11155)	Medium	2022.1.14638	CWE-79
IntelliJ IDEA	Insufficient notification about using Unicode directionality formatting characters (IDEA-284151)	Low	2022.1	CWE-176
IntelliJ IDEA	Local code execution via custom Pandoc path (IDEA-288269)	Medium	2022.1	CWE-94
IntelliJ IDEA	Local code execution via HTML descriptions in custom JSON schemas (IDEA-283967)	Medium	2022.1	CWE-94
IntelliJ IDEA	Local code execution via workspace settings (IDEA-283824, IDEA-283968)	Medium	2022.1	CWE-94
IntelliJ IDEA	HTML injection into IDE messages (IDEA-287428)	Low	2022.1	CWE-74
IntelliJ IDEA	Reflected XSS via error messages in internal web server (IDEA-283994)	Low	2022.1	CWE-79
IntelliJ IDEA	Flawed origin checks in the internal web server (IDEA-283586)	Low	2022.1	CWE-346

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	Local code execution via links in Quick Documentation (IDEA-289398)	Medium	2022.1	CWE-94
PyCharm	Exposure of the debugger port to the internal network (PY-52288)	Low	2022.1	CWE-1327
Rider	Local code execution via links in ReSharper Quick Documentation (RIDER-74099)	Medium	2022.1	CWE-94
TeamCity Cloud	Potential disclosure of built-in OAuth2 connectors' secrets. Reported by Yurii Sanin (TCC-346)	High	Not applicable	CWE-522
TeamCity Cloud	Session takeover via OAuth client manipulation. Reported by Yurii Sanin (TCC-347, TCC-349, TCC-351)	High	Not applicable	CWE-345
TeamCity Cloud	Session takeover using open redirect misconfiguration. Reported by Yurii Sanin (TCC-348)	High	Not applicable	CWE-601
TeamCity Cloud	VCS credentials disclosure via repository URL manipulation. Reported by Yurii Sanin (TCC-355, TCC-358)	Medium	Not applicable	CWE-522

Product	Description	Severity	Resolved In	CWE
Ktor	Random values used for nonce generation in Ktor Native weren't using SecureRandom implementations. Reported by Dan Wallach (KTOR-3656, Pull Request)	Low	2.0.0	CWE-330
JetBrains Account	It was possible to take over accounts linked to outlook.* email addresses via GitHub SSO. Reported by Adrian Weber (JPF-12877)	Critical	2022.04	CWE-697
IntelliJ IDEA	It was possible to get passwords from protected fields (IDEA-289085)	High	2021.3.3	CWE-497
YouTrack	HTML code from the issue description was being rendered (JT-58282)	Medium	2022.1.43563	CWE-80
YouTrack	It was possible to include an iframe from a third-party domain in the issue description (JT-68626)	Medium	2022.1.43563	CWE-1021
YouTrack	It was possible to inject JavaScript into Markdown in the YouTrack Classic UI (JT-68622)	High	2022.1.43700	CWE-79
Hub	Blind Server-Side Request Forgery (SSRF). Reported by Yurii Sanin (HUB-11052)	Medium	2021.1.14276	CWE-918

Product	Description	Severity	Resolved In	CWE
Hub	Reflected XSS. Reported by Yurii Sanin (HUB-10971)	Medium	2021.1.14276	CWE-79
Hub	SAML request takeover. Reported by Yurii Sanin (HUB-10978)	High	2022.1.14434	CWE-345
JetBrains Blog	Reflected XSS via tag parameter (BLOG-55)	Medium	Not applicable	CWE-79
JetBrains Marketplace	Stored XSS via plugin fields (MP-4190, MP-4191, MP-4192, MP-4196, MP-4201)	Medium	Not applicable	CWE-79
Kotlin Website	Clickjacking at talkingkotlin.com (KTL-84)	Low	Not applicable	CWE-1021
TeamCity	Reflected XSS (TW-74044)	Medium	2021.2.2	CWE-79
TeamCity	OS command injection in the Agent Push feature configuration. Reported by Cristian Chavez (TW-74822)	High	2021.2.3	CWE-78
TeamCity	Environmental variables of "password" type could be logged in some cases (TW-74625)	Medium	2021.2.3	CWE-532

Product	Description	Severity	Resolved In	CWE
YouTrack	SSTI via FreeMarker templates. Reported by Matei "Mal" Badanoiu (JT-68075)	High	2021.4.40426	CWE-1336
Hub	JetBrains Account integration exposed API keys with excessive permissions. Reported by Yurii Sanin (HUB-10958)	High	2021.1.13890	CWE-732
Hub	An unprivileged user could perform a DoS. Reported by Yurii Sanin (HUB-10976)	High	2021.1.13956	CWE-74
IntelliJ IDEA	Code could be executed without the user's permission on opening a project (IDEA-243002, IDEA-277306, IDEA-282396, IDEA-275917)	Medium	2021.2.4	CWE-345
IntelliJ IDEA	Potential LCE via RLO (Right-to-Left Override) characters (IDEA-284150)	Medium	2021.3.1	CWE-176
JetBrains Blog	Blind SQL injection. Reported by Khan Janny (BLOG-45)	Medium	Not applicable	CWE-89
Kotlin	No ability to lock dependencies for Kotlin Multiplatform Gradle projects. Reported by Carter Jernigan (KT-49449)	Medium	1.6.0	CWE-667

Product	Description	Severity	Resolved In	CWE
Kotlin Website	Clickjacking at kotlinlang.org (KTL-588)	Medium	Not applicable	CWE-1021
Remote Development	Unexpected open port on backend server. Reported by Damian Gwiżdż (GTW-894)	High	2021.3.1	CWE-1327
Space	Missing permission check in an HTTP API response (SPACE-15991)	High	Not applicable	CWE-284
TeamCity	A redirect to an external site was possible (TW-71113)	Low	2021.2.1	CWE-601
TeamCity	Logout failed to remove the "Remember Me" cookie (TW-72969)	Low	2021.2	CWE-613
TeamCity	GitLab authentication impersonation. Reported by Christian Pedersen (TW-73375)	High	2021.1.4	CWE-285
TeamCity	The "Agent push" feature allowed any private key on the server to be selected (TW-73399)	Low	2021.2.1	CWE-284
TeamCity	Blind SSRF via an XML-RPC call. Reported by Artem Godin (TW-73465)	Medium	2021.2	CWE-918
TeamCity	Time-of-check/Time-of-use (TOCTOU) vulnerability in agent registration via XML-RPC.	High	2021.2	CWE-367

Product	Description	Severity	Resolved In	CWE
	Reported by Artem Godin (TW-73468)			
TeamCity	An unauthenticated attacker could cancel running builds via an XML-RPC request to the TeamCity server. Reported by Artem Godin (TW-73469)	Medium	2021.2.1	CWE-284
TeamCity	Pull-requests' health items were shown to users without appropriate permissions (TW-73516)	Low	2021.2	CWE-284
TeamCity	Stored XSS. Reported by Yurii Sanin (TW-73737)	Medium	2021.2.1	CWE-79
TeamCity	URL injection leading to CSRF. Reported by Yurii Sanin (TW-73859)	Medium	2021.2.1	CWE-352
TeamCity	Changing a password failed to terminate sessions of the edited user (TW-73888)	Low	2021.2.1	CWE-613
TeamCity	XXE during the parsing of a configuration file (TW-73932)	Medium	2021.2.1	CWE-611
TeamCity	Reflected XSS (TW-74043)	Medium	2021.2.1	CWE-79

Product	Description	Severity	Resolved In	CWE
YouTrack	Stored XSS on the Notification templates page (JT-65752)	Low	2021.4.31698	CWE-79
YouTrack	A custom logo could be set with read-only permissions (JT-66214)	Low	2021.4.31698	CWE-284
YouTrack	Stored XSS via project icon. Reported by Yurii Sanin (JT-67176)	Medium	2021.4.36872	CWE-79
Datalore	Server version disclosure. Reported by Bharat (DL-9447)	Low	2021.3	CWE-209
Hub	Information disclosure via avatars metadata (HUB-10154)	Low	2021.1.13690	CWE-200
Hub	Potential DOS via user information. Reported by Bharat (HUB-10804)	Low	2021.1.13415	CWE-20
Hub	Stored XSS. Reported by Dmitry Sherstoboev (HUB-10854)	Medium	2021.1.13690	CWE-79
Hub	Authentication throttling mechanism could be bypassed. Reported by Bharat (HUB-10869)	Medium	2021.1.13690	CWE-180
JetBrains Account	Authentication throttling mechanism could be bypassed. Reported by Bharat (JPF-11933)	Medium	2021.07	CWE-180

Product	Description	Severity	Resolved In	CWE
Ktor	Improper nonce verification during OAuth2 authentication process. Reported by Ole Schilling Tjensvold (KTOR-3091)	Medium	1.6.4	CWE-303
Space	Authentication throttling mechanism could be bypassed. Reported by Bharat (SPACE-15282)	Low	Not applicable	CWE-180
Space	SSRF disclosing EC2 metadata (SPACE-15666)	High	Not applicable	CWE-918
TeamCity	User enumeration was possible (TW-70167)	Low	2021.1.2	CWE-200
TeamCity	RCE in agent push functionality. Reported by Eduardo Castellanos (TW-70384)	High	2021.1.2	CWE-78
TeamCity	Information disclosure via Docker Registry connection dialog (TW-70459)	Medium	2021.1	CWE-200
TeamCity	Some HTTP Security Headers were missed (TW-71376)	Low	2021.1.2	CWE-693
TeamCity	Email notifications could include unescaped HTML (TW-71981)	Low	2021.1.2	CWE-116
TeamCity	Insufficient permissions checks in create patch	Low	2021.1.2	CWE-285

Product	Description	Severity	Resolved In	CWE
	functionality (TW-71982)			
TeamCity	Stored XSS (TW-72007)	Low	2021.1.2	CWE-79
TeamCity	Insufficient permissions checks in agent push functionality (TW-72177)	Low	2021.1.2	CWE-285
TeamCity	X-Frame-Options Header was missed in some cases (TW-72464)	Low	2021.1.3	CWE-693
TeamCity	A newly created project could take settings from already deleted project (TW-72521)	Medium	2021.1.3	CWE-459
TeamCity Cloud	Session takeover using open redirect in OAuth integration. Reported by Yurii Sanin (TCC-277)	High	Not applicable	CWE-601
YouTrack	Stored XSS (JT-63483)	Low	2021.3.21051	CWE-79
YouTrack	Host header injection. Reported by Artem Ivanov (JT-65590)	Medium	2021.3.23639	CWE-601
YouTrack	Stored XSS. Reported by Artem Ivanov (JT-65749)	High	2021.3.24402	CWE-79
YouTrack InCloud	Unsafe EC2 configuration in YouTrack InCloud (JT-	Low	Not applicable	CWE-16

Product	Description	Severity	Resolved In	CWE
	63693, JT-63695)			
YouTrack Mobile	Client-side caching on iOS (YTM-12961)	Low	2021.2	CWE-524
YouTrack Mobile	Incomplete access tokens protection in iOS (YTM-12962, YTM-12965, YTM-12966)	Low	2021.2	CWE-311
YouTrack Mobile	Incomplete access tokens protection in Android (YTM-12964)	Low	2021.2	CWE-311
YouTrack Mobile	Task Hijacking in Android (YTM-12967)	Low	2021.2	CWE-287
YouTrack Mobile	iOS URL Scheme hijacking (YTM-12968)	Low	2021.2	CWE-287
YouTrack Mobile	Missing Security Screen on Android & iOS (YTM-12969)	Low	2021.2	CWE-287
Datalore	Potential JWT token takeover using redirect misconfiguration. Reported by Yurii Sanin (DL-9225, JPF-11801)	High	0.2.2	CWE-601
Datalore	There was no way to drop all active sessions. Reported by Bharat (DL-9247)	High	0.3.0	CWE-613

Product	Description	Severity	Resolved In	CWE
Hub	Potentially insufficient CSP for Widget deployment feature (JPS-10736)	Low	2021.1.13262	CWE-1021
Hub	Account takeover was possible during password reset. Reported by Viet Nguyen Quoc (JPS-10767)	High	2021.1.13402	CWE-601
Hub	HTML injection in the password reset email was possible. Reported by Bharat (JPS-10797)	Medium	2021.1.13402	CWE-79
JetBrains Account	OTP could be used several times after the successful validation (JPF-11119)	Low	2021.04	CWE-358
JetBrains Account	Potential account takeover via OAuth integration. Reported by Bharat (JPF-11802)	High	2021.06	CWE-918
JetBrains Website	Reflected XSS on jetbrains.com. Reported by Vasu Solanki (JS-14004)	Low	Not applicable	CWE-79
RubyMine	Code execution without user confirmation was possible for untrusted projects (RUBY-27702)	Medium	2021.1.1	CWE-345
Space	Deprecated organization-wide package repositories were publicly visible (SPACE-14151)	High	Not applicable	CWE-284

Product	Description	Severity	Resolved In	CWE
TeamCity	Potential XSS (TW-61688)	High	2020.2.3	CWE-79
TeamCity	Insecure deserialization (TW-70057, TW-70080)	High	2020.2.4	CWE-502
TeamCity	Insufficient authentication checks for agent requests (TW-70166)	High	2021.1.1	CWE-287
TeamCity	Insecure key generation for encrypted properties (TW-70201)	Low	2021.1	CWE-335
TeamCity	Insufficient checks during file uploading (TW-70546)	Medium	2020.2.4	CWE-434
TeamCity	Passwords in plain text sometimes could be stored in VCS (TW-71008)	Medium	2021.1	CWE-540
YouTrack	Insufficient sandboxing in workflows (JT-63222, JT-63254)	Critical	2021.1.11111	CWE-648
YouTrack	Time-unsafe comparisons were used (JT-63697)	Low	2021.2.16363	CWE-208
YouTrack	System user passwords were hashed with SHA-256 (JT-63698)	Low	2021.2.16363	CWE-916

Product	Description	Severity	Resolved In	CWE
YouTrack	Insecure PRNG was used (JT-63699)	Low	2021.2.16363	CWE-338
YouTrack	Stored XSS (JT-64564)	Medium	2021.2.17925	CWE-79
YouTrack	User could see boards without having corresponding permissions (JT-64634)	Low	2021.3.21051	CWE-284
YouTrack InCloud	Reflected XSS on konnector service in Firefox (JT-63702)	Low	Not applicable	CWE-79
Code With Me	Client could execute code in read-only mode (CWM-1235)	Medium	Compatible IDEs 2021.1 version	CWE-285
Code With Me	Client could open browser on host (CWM-1769)	Low	Compatible IDEs 2021.1 version	CWE-285
Exception Analyzer	No throttling at Exception Analyzer login page. Reported by Ashhad Ali (EXA-760)	Low	Not applicable	CWE-799
Hub	Two-factor authentication wasn't enabled properly for "All Users" group (JPS-10694)	Low	2021.1.13079	CWE-304

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	XXE in License server functionality (IDEA-260143)	High	2020.3.3	CWE-611
IntelliJ IDEA	Code execution without user confirmation was possible for untrusted projects (IDEA-260911, IDEA-260912, IDEA-260913, IDEA-261846, IDEA-261851, IDEA-262917, IDEA-263981, IDEA-264782)	Medium	2020.3.3	CWE-345
IntelliJ IDEA	Possible DoS. Reported by Arun Malik (IDEA-261832)	Medium	2021.1	CWE-770
JetBrains Academy	Potential takeover of a future account with a known email. Reported by Vansh Devgan (JBA-110)	Low	Not applicable	CWE-285
JetBrains Account	Sensitive account URLs were shared with third parties. Reported by Vikram Naidu (JPF-11338)	High	2021.02	CWE-201
JetBrains Website	Reflected XSS at blog.jetbrains.com. Reported by Peter Af Geijerstam and Jai Kumar (JS-14554, JS-14562)	Low	Not applicable	CWE-79
PyCharm	Code execution without user confirmation was possible for untrusted	Medium	2020.3.4	CWE-345

Product	Description	Severity	Resolved In	CWE
	projects. Reported by Tony Torralba (PY-41524)			
Space	Insufficient CRLF sanitization in user input (SPACE-13955)	Low	Not applicable	CWE-93
TeamCity	Potential XSS on the test history page (TW-67710)	Medium	2020.2.2	CWE-79
TeamCity	TeamCity IntelliJ Plugin DOS. Reported by Jonathan Leitschuh (TW-69070)	Low	2020.2.2	CWE-770
TeamCity	Local information disclosure via temporary file in TeamCity IntelliJ Plugin. Reported by Jonathan Leitschuh (TW-69420)	Low	2020.2.2	CWE-378
TeamCity	Insufficient audit when an administrator uploads a file (TW-69511)	Low	2020.2.2	CWE-778
TeamCity	Improper permission checks for changing TeamCity plugins (TW-69521)	Low	2020.2.2	CWE-732
TeamCity	Potential XSS on the test page. Reported by Stephen Patches (TW-69737)	Low	2020.2.2	CWE-79

Product	Description	Severity	Resolved In	CWE
TeamCity	Argument Injection leading to RCE (TW-70054)	High	2020.2.3	CWE-78
TeamCity	Stored XSS on several pages (TW-70078, TW-70348)	Medium	2020.2.3	CWE-79
TeamCity	Information disclosure via SSRF (TW-70079)	High	2020.2.3	CWE-918
TeamCity	Reflected XSS on several pages (TW-70093, TW-70094, TW-70095, TW-70096, TW-70137)	Medium	2020.2.3	CWE-79
TeamCity	Potential account takeover during password reset (TW-70303)	Medium	2020.2.3	CWE-640
TeamCity	Insufficient checks of the redirect_uri during GitHub SSO token exchange (TW-70358)	Low	2020.2.3	CWE-601
TeamCity	Arbitrary code execution on TeamCity Server running on Windows. Reported by Chris Moore (TW-70512)	High	2020.2.4	CWE-829
TeamCity	Command injection leading to RCE. Reported by Chris Moore (TW-70541)	High	2020.2.4	CWE-78

Product	Description	Severity	Resolved In	CWE
TeamCity Cloud	Potential information disclosure via EC2 instance metadata (TCC-174, TCC-176)	Low	Not applicable	CWE-1230
TeamCity Cloud	Temporary credentials disclosure via command injection. Reported by Chris Moore (TCC-196)	High	Not applicable	CWE-78
UpSource	Application passwords were not revoked correctly. Reported by Thibaut Zonca (UP-10843)	High	2020.1.1883	CWE-459
WebStorm	HTTP requests were used instead of HTTPS (WEB-49549)	Low	2021.1	CWE-295
WebStorm	Code execution without user confirmation was possible for untrusted projects (WEB-49689, WEB-49902)	Low	2021.1	CWE-345
YouTrack	Stored XSS via attached file. Reported by Mikhail Klyuchnikov (JT-62530)	Medium	2020.6.6441	CWE-79
YouTrack	Pull request title was sanitized insufficiently (JT-62556)	Medium	2021.1.9819	CWE-79
YouTrack	Improper access control during exporting issues (JT-62649)	High	2020.6.6600	CWE-284

Product	Description	Severity	Resolved In	CWE
YouTrack	Information disclosure in issue preview (JT-62919)	High	2020.6.8801	CWE-200
Code With Me	An attacker in the local network knowing session id could get access to the encrypted traffic. Reported by Grigorii Liullin (CWM-1067)	Low	2020.3	Not applicable
Datalore	Server components versions were disclosed (DL-8327, DL-8335)	Low	0.0.1	CWE-200
Exception Analyzer	Information disclosure via Exceptions Analyzer (SDP-1248)	Low	Not applicable	CWE-200
Hub	Open-redirect was possible. Reported by Mohammed Amine El Attar (JPS-10348)	Medium	2020.1.12629	Not applicable
Hub	Authorized user can delete 2FA settings of any other user (JPS-10410)	Medium	2020.1.12629	Not applicable
Hub	Information disclosure via public API (JPS-10481)	Low	2020.1.12669	Not applicable
IntelliJ IDEA	HTTP links were used for several remote repositories (IDEA-228726)	Low	2020.2	Not applicable

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	Potentially insecure deserialization of the workspace model (IDEA-253582)	Low	2020.3	Not applicable
JetBrains Account	Authorization token was sent as a query parameter within Zendesk integration (JPF-10508)	Low	2020.11	CWE-598
JetBrains Account	Open-redirect was possible (JPF-10660)	Low	2020.10	CWE-601
JetBrains Website	Cross-origin resource sharing was possible. Reported by Ashhad Ali (SDP-1193)	Low	Not applicable	CWE-942
JetBrains Website	Throttling was not used for the particular endpoint. Reported by Ashhad Ali (SDP-1197)	Low	Not applicable	CWE-799
JetBrains Website	Clickjacking was possible. Reported by Ashhad Ali (SDP-1203)	Low	Not applicable	CWE-1021
Kotlin	Vulnerable Java API was used for temporary files and folders creation, which could make temporary files available for other users of a system. Reported by Jonathan Leitschuh (KT-42181)	Low	1.4.21	Not applicable

Product	Description	Severity	Resolved In	CWE
Ktor	Birthday attack on SessionStorage key was possible. Reported by Kenta Koyama (KTOR-878)	Low	1.5.0	Not applicable
Ktor	Weak cipher suites were enabled by default. Reported by Johannes Ulfkjær Jensen (KTOR-895)	Low	1.4.2	Not applicable
Ktor	HTTP Request Smuggling was possible. Reported by ZeddYu Lu, Kaiwen Shen, Yaru Yang (KTOR-1116)	Low	1.4.3	Not applicable
PhpStorm	Source code could be added to debug logs (WI-54619)	Low	2020.3	Not applicable
Space	Potential information disclosure via logs (SPACE-9343, SPACE-10969)	Low	Not applicable	CWE-532
Space	An attacker could obtain limited information via SSRF in repository mirroring test connection (SPACE-9514)	High	Not applicable	CWE-918
Space	Content-Type header wasn't set for some pages (SPACE-12004)	Low	Not applicable	CWE-531
Space	REST API endpoint was available without appropriate permissions	Low	Not applicable	CWE-732

Product	Description	Severity	Resolved In	CWE
	check, which could introduce a potential DOS vector (no real exploit available). (SPACE-12288)			
TeamCity	Reflected XSS on several pages (TW-67424, TW-68098)	Medium	2020.2	Not applicable
TeamCity	TeamCity server DoS was possible via server integration (TW-68406, TW-68780)	Low	2020.2.2	Not applicable
TeamCity	ECR token exposure in the build's parameters (TW-68515)	Medium	2020.2	Not applicable
TeamCity	User could get access to GitHub access token of another user (TW-68646)	Low	2020.2.1	Not applicable
TeamCity	Server admin could create and see access tokens for any other users (TW-68862)	Low	2020.2.1	Not applicable
TeamCity	Improper permissions checks during user deletion (TW-68864)	Low	2020.2.1	Not applicable
TeamCity	Improper permissions checks during tokens removal (TW-68871)	Low	2020.2.1	Not applicable
TeamCity	TeamCity Plugin SSRF. Vulnerability that could potentially expose user	High	2020.2.85695	Not applicable

Product	Description	Severity	Resolved In	CWE
	credentials. Reported by Jonathan Leitschuh (TW-69068)			
YouTrack	CSRF via attachment upload. Reported by Yurii Sanin (JT-58157)	Medium	2020.4.4701	Not applicable
YouTrack	Users enumeration via REST API without appropriate permissions (JT-59396, JT-59498)	Low	2020.4.4701	Not applicable
YouTrack	Improper resource access checks (JT-59397)	Low	2020.4.4701	Not applicable
YouTrack	Issue's existence disclosure via the YouTrack command execution (JT-59663)	Low	2020.6.1767	Not applicable
YouTrack	Improper permissions checks for the attachments actions (JT-59900)	Low	2020.4.4701	Not applicable
YouTrack	YouTrack admin wasn't able to access attachments (JT-60824)	Low	2020.4.6808	Not applicable
YouTrack	Server-side template injection in the YouTrack Cloud. Reported by Vasily Vasilkov (JT-61449)	High	2020.5.3123	Not applicable
YouTrack	Project information disclosure (JT-61566)	Low	2020.6.1099	Not applicable

Product	Description	Severity	Resolved In	CWE
IdeaVim	In limited circumstances, IdeaVim might have caused information leak (VIM-2019)	High	0.58	Not applicable
IntelliJ IDEA	Built-in web server could expose information about IDE version (IDEA-240567)	Low	2020.2	Not applicable
JetBrains Account	Improper rate limit. Reported by Ashhad Ali (JPF-11026)	Low	2020.09	CWE-799
JetBrains Account	Password reset token might be disclosed to a third party. Reported by Sheikh Rishad (JPF-11034)	Low	2020.10	CWE-201
JetBrains Marketplace	Blind SSRF. Reported by Yurii Sanin (MP-3119)	High	Not applicable	CWE-918
JetBrains Website	Reflected XSS. Reported by Peter af Geijerstam (JS-13032)	Medium	Not applicable	CWE-79
JetBrains Website	HTML injection was possible on several pages (JS-13041)	Medium	Not applicable	CWE-79
JetBrains Website	Clickjacking was possible on several pages (JS-13042)	Low	Not applicable	CWE-1021
JetBrains Website	SSRF on the website. Reported by Mohamed Lahraoui (SDP-1174)	Low	Not applicable	CWE-918

Product	Description	Severity	Resolved In	CWE
Ktor	HTTP request smuggling was possible. Reported by ZeddYu Lu and Kaiwen Shen (KTOR-841)	Medium	1.4.1	Not applicable
Space	Unauthorized access to environment variables containing private data (SPACE-10723)	Medium	Not applicable	CWE-532
TeamCity	URL injection was possible (TW-44171)	Low	2020.1.2	Not applicable
TeamCity	Guest user had access to audit records (TW-67750)	Medium	2020.1.5	Not applicable
TeamCity	Secure dependency parameters could be not masked in depending builds when there are no internal artifacts (TW-67775)	High	2020.1.5	Not applicable
Toolbox App	Limited RCE via jetbrains protocol handler. Reported by Jeffrey van Gogh and Yuriy Solodkyy (SDP-1177)	Low	1.18	Not applicable
Toolbox App	Denial of service via jetbrains protocol handler (TBX-5281)	Low	1.18.7455	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Blind SSRF. Reported by Yurii Sanin (JT-58015)	Low	2020.3.888	Not applicable
YouTrack	Notifications might have mentioned inaccessible issues (JT-58329)	Low	2020.3.888	Not applicable
YouTrack	SSRF in YouTrack InCloud. Reported by Yurii Sanin (JT-58962)	Medium	2020.3.5333	Not applicable
YouTrack	Improper access control allowed retrieving issue description without appropriate access. Reported by Yurii Sanin (JT-59015)	Critical	2020.3.4313, 2020.2.11008, 2020.1.11011, 2019.3.65516, 2019.2.65515, 2019.1.65514	Not applicable
YouTrack	Improper access control for some subresources leads to information disclosure. Reported by Yurii Sanin (JT-59130)	Medium	2020.3.6638	Not applicable
YouTrack	An attacker could access workflow rules without appropriate access grants (JT-59474)	High	2020.3.7955	Not applicable
YouTrack Mobile	Information disclosure via application backups. Reported by Cristi Vlad (YTM-5518)	Low	2020.2.0	Not applicable
Datalore	Stack trace disclosure. (DL-7350)	Low	0.0.1	CWE-536

Product	Description	Severity	Resolved In	CWE
Datalore	Reverse tabnabbing was possible. (DL-7708)	Low	0.0.1	CWE-1022
JetBrains Account	Missed throttling for reset password functionality in case of 2FA enabled. Reported by Manu Pranav. (JPF-10527)	Medium	2020.06	CWE-799
JetBrains Website	Stack trace disclosure in case of incorrect character in request. (JS-12490)	Low	Not applicable	CWE-536
JetBrains Website	Reflected XSS on jetbrains.com subdomain. Reported by Ritik Chaddha. (JS-12562)	Low	Not applicable	CWE-79
JetBrains Website	Open-redirect issues on kotlinconf.com. Reported by Ritik Chaddha. (JS-12581)	Low	Not applicable	CWE-601
JetBrains Website	Clickjacking was possible at a non-existent page. Reported by Pravas Ranjan Kanungo. (JS-12835)	Low	Not applicable	CWE-1021
Kotlin	Script cache privilege escalation vulnerability. Reported by Henrik Tunedal. (KT-38222)	Medium	1.4.0	Not applicable
Space	Draft title was disclosed to a user without access to the draft. (SPACE-5594)	Low	Not applicable	CWE-200

Product	Description	Severity	Resolved In	CWE
Space	Missing authorisation check caused privilege escalation. Reported by Callum Carney. (SPACE-8034)	High	Not applicable	CWE-266
Space	Blind SSRF via calendar import. Reported by Yurii Sanin. (SPACE-8273)	Medium	Not applicable	CWE-918
Space	The drafts of the direct messages sent from iOS app could be sent to the channel. (SPACE-8377)	Low	Not applicable	CWE-200
Space	Chat messages are propagated to the browser console. (SPACE-8386)	High	Not applicable	CWE-215
Space	Missed authentication checks in Space Automation. (SPACE-8431)	Critical	Not applicable	CWE-306
Space	Missed authentication checks in Job related API. (SPACE-8822)	Low	Not applicable	CWE-306
Space	Incorrect checks of public key content. (SPACE-9169)	Medium	Not applicable	CWE-287
Space	Stored XSS via repository resource. (SPACE-9277)	High	Not applicable	CWE-79

Product	Description	Severity	Resolved In	CWE
TeamCity	Users were able to assign more permissions than they had. (TW-36158)	Low	2020.1	Not applicable
TeamCity	Users with "Modify group" permission can elevate other users privileges. (TW-58858)	Medium	2020.1	Not applicable
TeamCity	Password parameters could be disclosed via build logs. (TW-64484)	Low	2019.2.3	Not applicable
TeamCity	Project parameter values could be retrieved by a user without appropriate permissions. (TW-64587)	High	2020.1.1	Not applicable
TeamCity	Reflected XSS on administration UI. (TW-64668)	High	2019.2.3	Not applicable
TeamCity	Stored XSS on administration UI. (TW-64699)	High	2019.2.3	Not applicable
Toolbox App	Missed signature on "jetbrains-toolbox.exe". (TBX-4671)	Low	1.17.6856	Not applicable
UpSource	Unauthorised access was possible through error in accounts linking. (SDP-940)	Low	2020.1	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Subtasks workflow could disclose issue existence. (JT-45316)	Low	2020.2.8527	Not applicable
YouTrack	An external user could execute commands against arbitrary issues. (JT-56848)	High	2020.1.1331	Not applicable
YouTrack	SSRF vulnerability that allowed scanning internal ports. Reported by Evren Yalçın. (JT-56917)	Low	2020.2.10643	Not applicable
YouTrack	Markdown parser could disclose hidden file existence. (JT-57235)	Low	2020.2.6881	Not applicable
YouTrack	A user without permission was able to create articles draft. (JT-57649)	Medium	2020.2.6881	Not applicable
YouTrack	AWS metadata of YouTrack InCloud instance disclosure via SSRF in Workflow. Reported by Yurii Sanin. (JT-57964)	High	2020.2.8873	Not applicable
YouTrack	SSRF was possible due to the fact that URL filtering could be escaped. Reported by Yurii Sanin. (JT-58204)	Low	2020.2.10514	Not applicable
YouTrack InCloud	Possibility to change redirect from any existing YouTrack InCloud instance	Medium	2020.1.3588	CWE-601

Product	Description	Severity	Resolved In	CWE
	to other instance. (JT-57036)			
Datalore	User's SSH key can be deleted without appropriate permissions. Reported by Callum Carney (DL-7833)	Medium	0.0.1	CWE-639
Datalore	SSRF could be caused by an attached file. Reported by Callum Carney (DL-7836)	High	0.0.1	CWE-918
GoLand	Plain HTTP was used to access plugin repository (GO-8694)	Low	2019.3.2	Not applicable
Hub	Content spoofing at Hub OAuth error message was possible (JPS-10093)	Medium	2020.1.12099	Not applicable
IntelliJ IDEA	License server could be resolved to untrusted host in some cases (IDEA-219748)	High	2020.1	Not applicable
JetBrains Account	Non-unique QR codes were generated during consequentattempts to setup 2FA (JPF-10149)	Low	2020.01	CWE-342
JetBrains Account	Clickjacking was possible on a JetBrains Account page. Reported by Raja Ahtisham (JPF-10154)	Medium	2020.01	CWE-1021

Product	Description	Severity	Resolved In	CWE
JetBrains Account	Customer name enumeration by numeric customer ID was possible (JPF-10159, JPF-10301)	High	2020.03	CWE-200
JetBrains Account	Country value coming from a user wasn't correctly validated (JPF-10258)	High	2020.02	CWE-285
JetBrains Account	Information disclosure from JetBrains Account was possible via "Back" button. Reported by Ratnadip Gajbhiye (JPF-10266)	Low	2020.02	CWE-200
JetBrains Marketplace	Uploading malicious file via Screenshots form could cause XSS (MP-2637)	Medium	Not applicable	CWE-79
JetBrains Website	Reflected XSS at jetbrains.com was possible. Reported by Rahad Chowdhury (JS-11769)	High	Not applicable	CWE-79
PyCharm	Apple Notarization Service credentials were included to PyCharm distributive for Windows reported by Ruby Nealon (IDEA-232217)	High	2019.3.3, 2019.2.6	Not applicable

Product	Description	Severity	Resolved In	CWE
Space	Session timeout period was configured improperly (SPACE-4717)	Low	Not applicable	Not applicable
Space	Stored XSS in Space chats was possible. Reported by Callum Carney (SPACE-6556)	Medium	Not applicable	Not applicable
Space	Password authentication implementation was insecure (SPACE-7282)	High	Not applicable	Not applicable
TeamCity	Passwords values were shown not being masked on several pages (TW-64186)	Low	2019.2.2	Not applicable
TeamCity	Project administrator was able to see scrambled password parameters used in a project (TW-58099)	Medium	2019.2.2	Not applicable
TeamCity	Project administrator was able to retrieve some TeamCity server settings (TW-61626)	Low	2019.1.4	Not applicable
TeamCity	Application state kept alive after a user ends his session (TW-61824)	Low	2019.2.1	Not applicable
TeamCity	A user without appropriate permissions was able import settings from settings.kts (TW-63698)	Low	2019.2.1	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	DB export was accessible to read-only administrators (JT-56001)	Low	2020.1.659	Not applicable
YouTrack	DoS could be performed by attaching malformed TIFF to an issue. Reported by Chris Smith (JT-56407)	High	2020.1.659	Not applicable
IDETalk plugin	XXE in IDETalk plugin. (IDEA-220136 reported by Srikanth Ramu)	Medium	193.4099.10	Not applicable
IntelliJ IDEA	Some Maven repositories are accessed via HTTP instead of HTTPs. (IDEA-216282)	High	2019.3	Not applicable
IntelliJ IDEA	Ports listened to by IntelliJ IDEA are exposed to the network. (IDEA-219695)	Low	2019.3	Not applicable
IntelliJ IDEA	XSLT debugger plugin misconfiguration allows arbitrary file read over network. (IDEA-216621 reported by Anatoly Korniltsev)	Medium	2019.3	Not applicable
JetBrains Account	Profile names are exposed by email. (JPF-9219 reported by Timon Birk)	Low	2019.11	CWE-200
JetBrains Account	Missing secure flag for cookie. (JPF-9857)	Low	2019.11	CWE-614

Product	Description	Severity	Resolved In	CWE
JetBrains Account	Insufficient authentication on contact view. (JPF-10024)	High	2019.11	CWE-287
JetBrains Account	Insufficient authentication on role update. (JPF-10025)	High	2019.11	CWE-287
JetBrains Account	XSS on the spending report page. (JPF-10027)	Medium	2019.12	CWE-79
JetBrains Account	Open redirect during re-acceptance of license agreements. (JPF-10028)	Low	2019.11	CWE-601
JetBrains Account	Information exposure during processing of license requests. (JPF-10111)	High	2019.12	CWE-200
JetBrains Marketplace	XSS on several pages. (MP-2617, MP-2640, MP-2642)	Low	Not applicable	CWE-79
JetBrains Marketplace	Improper access control during plugins upload. (MP-2695)	Critical	Not applicable	CWE-284
JetBrains Website	Cookie XSS at jetbrains.com. (JS-10969)	High	Not applicable	CWE-79
Ktor	The Ktor framework is vulnerable to HTTP Response Splitting. Reported by Jonathan Leitschuh	High	1.2.6	Not applicable

Product	Description	Severity	Resolved In	CWE
Ktor	The Ktor client resends authorization data to a redirect location. Reported by Jonathan Leitschuh	Low	1.2.6	Not applicable
Ktor	Request smuggling is possible when both chunked Transfer-Encoding and Content-Length are specified. Reported by Jonathan Leitschuh	Low	1.3.0	Not applicable
Rider	Unsigned binaries in Windows installer. (RIDER-30393)	Medium	2019.3	Not applicable
Scala plugin	Artifact dependencies were resolved over unencrypted connections. (SCL-15063)	High	2019.2.1	Not applicable
TeamCity	Reverse Tabnabbing is possible on several pages. (TW-61710, TW-61726, TW-61727)	Low	2019.1.5	Not applicable
TeamCity	Some server-stored passwords can be shown via web UI. (TW-62674)	High	2019.1.5	Not applicable
TeamCity	Possible stored XSS attack by a user with a developer role. (TW-63298)	Medium	2019.2	Not applicable

Product	Description	Severity	Resolved In	CWE
TeamCity	Stored XSS on user-level pages. (TW-63160)	High	2019.2	Not applicable
YouTrack	CORS misconfiguration on youtrack.jetbrains.com. (JT-53675)	Medium	Not applicable	CWE-346
YouTrack	SMTP/Jabber settings can be accessed using backups. (JT-54139)	Medium	2019.2.59309	Not applicable
YouTrack	XSS via image upload at youtrack-workflow-converter.jetbrains.com. (JT-54589)	Low	Not applicable	CWE-80
YouTrack	XSS via issue description. (JT-54719)	High	2019.2.59309	Not applicable
Hub	Username enumeration was possible through password recovery. JPS-9655, JPS-9938	Low	2019.1.11738	Not applicable
IntelliJ IDEA	Local user privilege escalation potentially allowed arbitrary code execution. IDEA-216623	Low	2019.2	Not applicable
JetBrains Account	Account removal without re-authentication was possible. JPF-9611 reported by Siamul Islam.	Medium	2019.9	CWE-306
JetBrains Account	Password reset link was not invalidated during password change through	Medium	2019.8	CWE-613

Product	Description	Severity	Resolved In	CWE
	profile. JPF-9610 reported by Elliot V. Daniel.			
MPS	Ports listened to by MPS are exposed to the network. MPS-30661	Low	2019.2.2	Not applicable
TeamCity	Access could be gained to the history of builds of a deleted build configuration under some circumstances. TW-60957	Medium	2019.1.2	Not applicable
TeamCity	Insecure Java Deserialization could potentially allow RCE. TW-61928 reported by Aleksei "GreenDog" Tiurin.	Medium	2019.1.4	Not applicable
TeamCity	Reverse tabnabbing was possible on several pages. TW-61323, TW-61725,TW-61726, TW-61646,TW-62123	Low	2019.1.4	Not applicable
TeamCity	Secure values could be exposed to users with the ‘View build runtime parameters and data’ permission.	Low	2019.1.2	Not applicable
TeamCity	A non-destructive operation could be performed by a user without the corresponding permissions. TW-61107	Low	2019.1.2	Not applicable

Product	Description	Severity	Resolved In	CWE
Toolbox App	Privilege escalation was possible in the JetBrains Toolbox App for Windows.TBX-3759	Low	1.15.5666	Not applicable
YouTrack	Removing tags from issues list without corresponding permission was possible. JT-53465	Low	2019.2.55152	Not applicable
YouTrack InCloud	Sending of arbitrary spam email from a Youtrack instance was possible. JT-54136, ADM-13823, ADM-34971	Low	Not applicable	CWE-285
Exception Analyzer	Insecure transfer of JetBrains Account credentials. EXA-652	Critical	Not applicable	CWE-598
Hub	No way to set a password to expire automatically. JPS-8816	Low	2018.4.11436	Not applicable
IdeaVim	Project data appeared in user level settings. VIM-1184	Medium	0.52	Not applicable
IntelliJ IDEA	Resolving artifacts using an http connection, potentially allowing an MITM attack. IDEA-211231	High	2019.2	Not applicable
JetBrains Account	Authorized account enumeration. JPF-9370	Low	2019.5	CWE-204

Product	Description	Severity	Resolved In	CWE
JetBrains Account	Cross-origin resource sharing misconfiguration (Reported by Vishnu Vardhan). JPF-9095	Low	2019.5	CWE-942
JetBrains Account	No rate limitation on the account details page. JPF-9704	Medium	2019.8	CWE-770
JetBrains Account	No rate limitation on the licenses page. JPF-9713	High	2019.9	CWE-770
JetBrains Account	Unauthorized disclosure of license email on the licenses page. JPF-9692	Critical	2019.8	CWE-284
JetBrains Website	Reflected XSS. JS-9853	Medium	Not applicable	CWE-79
Ktor	Command injection through LDAP username.	Medium	1.2.0-rc, 1.2.0	Not applicable
Ktor	Predictable Salt for user credentials.	Medium	1.2.0-rc2, 1.2.0	Not applicable
PyCharm	Remote call causing an “out of memory” error was possible. PY-35251	Low	2019.2	Not applicable
ReSharper	DLL hijacking vulnerability. RSRP-473674	High	2019.2	Not applicable

Product	Description	Severity	Resolved In	CWE
Rider	Unsigned DLL was used in a distributive. RIDER-27708	Medium	2019.1.2	Not applicable
TeamCity	Previously used unencrypted passwords were suggested by a web browser's auto-completion. TW-59759	Low	2019.1	CWE-200
TeamCity	VMWare plugin did not check SSL certificate. TW-59562	Medium	2019.1	Not applicable
TeamCity	Remote Code Execution on the server with certain network configurations. TW-60430	Medium	2019.1	Not applicable
TeamCity	Project administrator could get unauthorized access to server-level data. TW-60220	High	2019.1	Not applicable
TeamCity	Project administrator could execute any command on the server machine. TW-60219	High	2019.1	Not applicable
TeamCity	Security has been tightened thanks to using additional HTTP headers. TW-59034	High	2019.1	Not applicable
TeamCity	Possible XSS vulnerabilities on the settings pages. TW-59870, TW-59852, TW-	High	2019.1	Not applicable

Product	Description	Severity	Resolved In	CWE
	59817, TW-59838, TW-59816			
TeamCity	XSS vulnerability. TW-61242, TW-61315	High	2019.1.2	Not applicable
Toolbox App	Unencrypted connection to external resources, potentially allowed an MITM attack. TBX-3327, ADM-30275	Low	1.15.5605	CWE-311
UpSource	Insufficient escaping of code blocks. UP-10387	Medium	2019.1.1412	Not applicable
UpSource	Credentials exposure via RPC command. UP-10344	Critical	2018.2.1290	Not applicable
UpSource	Credentials exposure via RPC command. UP-10343	Critical	2018.2.1293	Not applicable
YouTrack	A user could get a list of project names under certain conditions. JT-53162	Low	2019.2.53938	Not applicable
YouTrack	Stored XSS via issue attachments. JT-51077	High	2019.2.53938	Not applicable
YouTrack	Stored XSS on the issue page. JT-54121	High	2019.2.56594	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Stored XSS in the issues list. JT-52894	High	2019.1.52584	Not applicable
YouTrack	A compromised URL was automatically whitelisted by YouTrack. JT-47653	Low	2019.1.52545	Not applicable
YouTrack	Cross-Site Request Forgery. JT-30098	Low	2019.1	Not applicable
CLion	The suggested WSL configuration exposed a local SSH server to the internal network. CPP-15063	Medium	Not applicable	CWE-276
Hub	A user password could appear in the audit events for certain server settings. JPS-7895	High	2018.4.11298	Not applicable
IntelliJ IDEA	The default configuration for Spring Boot apps was not secure. IDEA-204439	High	2018.3.4, 2019.1	Not applicable
IntelliJ IDEA	The application server configuration allowed cleartext storage of secrets. IDEA-201519, IDEA-202483, IDEA-203271	High	2018.1.8, 2018.2.8, 2018.3.5, 2019.1	Not applicable

Product	Description	Severity	Resolved In	CWE
IntelliJ IDEA	The implementation of storage in the KeePass database was not secure. IDEA-200066	Low	2018.3, 2019.1	CWE-922
IntelliJ IDEA	A certain application server configuration allowed cleartext storage of secrets. IDEA-199911	Low	2018.3	CWE-317
IntelliJ IDEA	A certain application server configuration allowed cleartext storage of secrets. IDEA-203613	Medium	2018.1.8, 2018.2.8, 2018.3.5	Not applicable
IntelliJ IDEA	A certain remote server configurations allowed cleartext storage of secrets. IDEA-203272, IDEA-203260, IDEA-206556, IDEA-206557	High	2019.1	Not applicable
IntelliJ IDEA	The run configuration of certain application servers allowed remote code execution while running the server with the default settings. IDEA-204570	High	2017.3.7, 2018.1.8, 2018.2.8, 2018.3.4	Not applicable
JetBrains Account	An open redirect vulnerability via the backUrl parameter was detected. JPF-8899	Medium	Not applicable	CWE-601

Product	Description	Severity	Resolved In	CWE
JetBrains Account	The host header injection vulnerability was detected at account.jetbrains.com. ADM-20535	Medium	Not applicable	CWE-444
JetBrains Marketplace	Some HTTP Security Headers were missing. MP-2004	Medium	Not applicable	CWE-693
JetBrains Marketplace	A reflected XSS was detected. MP-2001	Medium	Not applicable	CWE-79
JetBrains Marketplace	A CSRF vulnerability was detected. MP-2002	Medium	Not applicable	CWE-352
JetBrains Website	A reflected XSS was detected. JT-51074	Low	Not applicable	CWE-79
Kotlin	The JetBrains Kotlin project was resolving artifacts using anhttp connection during the build process, potentially allowing an MITM attack.	Medium	1.3.30	Not applicable
Kotlin plugin for IntelliJ	IntelliJ IDEA projects created using the KotlinIDE template were resolving artifacts using an http connection, potentially allowing an MITM attack.	Medium	1.3.30	Not applicable
PyCharm	A certain remote server configuration allowed cleartext storage of secrets. PY-32885	Medium	2018.3.2	CWE-209

Product	Description	Severity	Resolved In	CWE
TeamCity	A possible stored JavaScript injection was detected. TW-59419	Medium	2018.2.3	Not applicable
TeamCity	The generated Kotlin DSL settings allowed usage of an unencrypted connection for resolving artifacts. TW-59379	Medium	2018.2.3	Not applicable
TeamCity	A possible stored JavaScript injection requiring a deliberate server administrator action was detected. TW-55640	Medium	2018.2.3	Not applicable
TeamCity	Incorrect handling of user input in ZIP extraction. TW-57143	Medium	2018.2.2	Not applicable
TeamCity	A reflected XSS on a user page was detected. TW-58661	Medium	2018.2.2	Not applicable
TeamCity	A user without the required permissions could gain access to some settings. TW-58571	Medium	2018.2.2	Not applicable
YouTrack	An SSRF attack was possible on a YouTrack server. JT-51121	High	2018.4.49168	Not applicable
YouTrack	An Insecure Direct Object Reference was possible. JT-51103	Low	2018.4.49168	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Certain actions could cause privilege escalation for issue attachments. JT-51080	Medium	2018.4.49168	Not applicable
YouTrack	A query injection was possible. JT-51105	Low	2018.4.49168	Not applicable
YouTrack	A CSRF vulnerability was detected in one of admin endpoints. JT-51110	Medium	2018.4.49852	Not applicable
YouTrack	The YouTrack Confluence plugin allowed the SSTI vulnerability. JT-51594	Medium	1.8.1.3	Not applicable
YouTrack InCloud	An unauthorized disclosure of license details to an attacker #2 was possible. JT-51117	Low	Not applicable	CWE-284
Hub	Admin account takeover of a system authorized with Hub was possible. JPS-9594	Critical	2018.3.11035	Not applicable
Hub	XXE was possible. JPS-9616, UP-10218	High	2018.4.11067	Not applicable
JetBrains Account	Disclosure of email address within unsuccessful login attempt. JPF-8663	High	4.11	Not applicable

Product	Description	Severity	Resolved In	CWE
TeamCity	Reflected XSS on user-level pages. TW-58065, TW-58234	High	2018.2	Not applicable
TeamCity	Stored XSS on the build details page. TW-58129, TW-58138	High	2018.2	Not applicable
TeamCity	Exposure of sensitive parameter value to a privileged user was possible. TW-56946	Medium	2018.1.3	Not applicable
UpSource	A privileged user had access to user credentials in rare case. UP-10092	Medium	2018.2.1141	Not applicable
YouTrack	Unauthorized access to project and user details with guest user banned was possible. JT-50970, JT-49827, JT-50611, JT-50203	High	2018.3.47010	Not applicable
YouTrack	Stored XSS on YouTrack issue page. JT-50201	Low	2018.3.47965	Not applicable
YouTrack InCloud	Unauthorized disclosure of YouTrack InCloud subscription information was possible. JPF-8714, JT-51001	High	2018.4.48293	Not applicable
YouTrack InCloud	Unauthorized access to the email address of YouTrack InCloud was possible. JT-50946	High	2018.4.48293	Not applicable

Product	Description	Severity	Resolved In	CWE
dotPeek	Remote Code Execution was possible while operating specific files. DOTP-7635	High	2018.1.4	Not applicable
Hub	Hub stored license information in log files. JPS-9187	Low	2018.2.10527	Not applicable
IntelliJ IDEA	Insecure connection used to access JetBrains resources. IDEA-187601, IDEA-192440	Medium	2018.1.5	Not applicable
IntelliJ IDEA	Incorrect handling of user input in ZIP extraction. IDEA-191679, IDEA-191680, IDEA-193358	High	2018.2	Not applicable
JetBrains Account	A few customer profiles were made available without authorization. JPF-8211	Medium	Not applicable	Not applicable
JetBrains Account	It was possible to obtain customer business email from order reference. JPF-7903	Medium	Not applicable	Not applicable
JetBrains Marketplace	XXE vulnerability. MP-1708	Low	Not applicable	Not applicable
JetBrains Marketplace	Incorrect handling of user input in ZIP extraction. MP-1678	Medium	Not applicable	Not applicable

Product	Description	Severity	Resolved In	CWE
ReSharper	Incorrect handling of user input in ZIP extraction. RSRP-470115	High	2018.1.3	Not applicable
TeamCity	CSRF vulnerability. TW-55992	Medium	2018.1.1	Not applicable
TeamCity	Change of project settings can corrupt settings of other projects. TW-55704	Low	2018.1.1	Not applicable
TeamCity	Possible privilege escalation while viewing agent details. TW-56025	Medium	2018.1.1	Not applicable
TeamCity	Possible unvalidated redirect. TW-56085	Medium	2018.1.2	Not applicable
TeamCity	Reflected XSS vulnerabilities. TW-56490, TW-56375, TW-56374	Medium	2018.1.2	Not applicable
TeamCity	Stored XSS vulnerabilities. TW-56830, TW-56719	Medium	2018.1.3	Not applicable
TeamCity	Stored XSS vulnerabilities. TW-55214, TW-56126, TW-56127, TW-56452, TW-56571	Medium	2018.1.2	Not applicable
YouTrack	Reflected XSS vulnerability. JT-48606	Medium	2018.2.45073	Not applicable
YouTrack	Possible privilege escalation via deprecated REST API. JT-48605	Low	2018.2.45073	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Possible tabnabbing via issue content. JT-47993	Low	2018.2.44329	Not applicable
Hub	ClickJacking vulnerability. JPS-7209	Low	2017.4.8040	Not applicable
Hub	ClickJacking vulnerability. JPS-8009	Low	2018.2.9541	Not applicable
IntelliJ IDEA	ROBOT attack vulnerability in certain subsystems. IDEA-183912	Low	2018.1.3	Not applicable
Scala plugin	Possible unauthenticated access to local compile server. SCL-13584	Medium	2018.2	Not applicable
TeamCity	Possible privilege escalation to server administrator. TW-55209	High	2018.1	Not applicable
TeamCity	CSRF attack vulnerability. TW-55210	High	2018.1	Not applicable
TeamCity	Possible privilege escalation from project administrator to server administrator. TW-55211, TW-55684	High	2018.1	Not applicable
TeamCity	Possible unauthorized removal of installation data by project administrator. TW-54876	High	2018.1	Not applicable
TeamCity	Network access to an agent allowed potential	Medium	2018.1	Not applicable

Product	Description	Severity	Resolved In	CWE
	unauthorized control over the agent. TW-49335			
TeamCity	In a very specific scenario, an attacker could steal web responses meant for other users. TW-54486	Medium	2018.1	Not applicable
TeamCity	Stored XSS vulnerabilities on various pages. TW-27206, TW-54129, TW-55453, TW-55215, TW-55217, TW-55353	Medium	2018.1	Not applicable
TeamCity	Project viewer could delete non-critical project settings. TW-55261	Medium	2018.1	Not applicable
TeamCity	Network access to a server allowed potential read access to project settings. TW-54870	Medium	2018.1	Not applicable
TeamCity	Project viewer could affect details of some running builds. TW-54975	Medium	2018.1	Not applicable
TeamCity	Reflected XSS vulnerabilities on various pages. TW-55212, TW-55213	Medium	2018.1	Not applicable
TeamCity	User self-registration might have been enabled by default on new server installation. TW-54741	Medium	2017.2.4, 2018.1	Not applicable

Product	Description	Severity	Resolved In	CWE
TeamCity	Possible vulnerability to ClickJacking attack from TeamCity UI. TW-33819	Medium	2017.2.4, 2018.1	Not applicable
TeamCity	Project viewer could bypass the "View build runtime parameters and data" permission. TW-55502	Low	2018.1	Not applicable
TeamCity	Network access to a server exposed a vulnerability to DoS attacks. TW-11984	Low	2018.1	Not applicable
TeamCity	Potential to pass authorization cookies without secure flags. TW-55141	Low	2018.1	Not applicable
UpSource	Vulnerability to ClickJacking attack. UP-9673	Medium	2018.1	Not applicable
UpSource	Possible privilege escalation during the configuration process. BND-1154, BND-1579, UP-7359. Reported by Zhiyong Feng from Mobike Security Team	Low	2018.1	Not applicable
YouTrack	Stored XSS vulnerabilities from specific pages. JT-47824	High	2018.2.42881	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	Potential for unauthorized users to view names of SSL keys. JT-47685	Low	2018.2.42881	Not applicable
YouTrack	Swimlane functionality allowed unauthorized changes to a limited number of issue properties. JT-47125	Low	2018.2.42133	Not applicable
dotTrace	dotTrace allowed privilege escalation (PROF-668)	Critical	2017.1, 2017.2, 2017.3, 2018.1	Not applicable
Hub	Limitation of login attempts at hub.jetbrains.com was disabled (JPS-7627)	Low	2018.1.9041	Not applicable
Hub	It was possible to obtain a new access token for a banned user (JPS-7553)	Low	2017.4.8440	Not applicable
IntelliJ IDEA	YourKit profiler port was available externally in EAP builds for Linux (IDEA-184795)	Low	2018.1	Not applicable
JetBrains Account	Privilege escalation was possible for JetBrains Account activity log (JPF-7437)	Medium	Not applicable	Not applicable
JetBrains Account	Valid password links might remain upon password reset (JPF-7335)	Low	Not applicable	Not applicable

Product	Description	Severity	Resolved In	CWE
TeamCity	VCS preview allowed XSS attack (TW-54027)	Medium	2017.2.3	Not applicable
TeamCity	Data Directory preview allowed XSS attack (TW-54021)	Low	2017.2.3	Not applicable
TeamCity	vmWare plugin settings allowed XSS attack (TW-53984)	High	2017.2.3	Not applicable
TeamCity	VCS settings allowed XSS attack (TW-53943, TW-53978)	High	2017.2.3	Not applicable
TeamCity	Authentication bypass was possible with certain Windows server configuration (TW-53507)	Medium	2017.2.2	Not applicable
TeamCity	Project administrator could run arbitrary code (TW-50054)	High	2017.2.2	Not applicable
TeamCity	Build fields allowed XSS attack (TW-53466)	Medium	2017.2.2	Not applicable
TeamCity	Multiple XSS vulnerabilities (reported by Viktor Gazdag of NCC Group) (TW-53442)	High	2017.2.2	Not applicable
UpSource	Multiple XSS vulnerabilities (Reported by Viktor Gazdag of NCC Group) (UP-9606)	Medium	2017.3.2888	Not applicable

Product	Description	Severity	Resolved In	CWE
YouTrack	RSS feed allowed unauthorized access to comments with certain configuration (JT-46375)	Medium	2018.1.40341	Not applicable
YouTrack	REST API allowed unauthorized access to attachments of hidden comments (JT-46004)	Medium	2018.1.40341	Not applicable
YouTrack	RSS feed allowed unauthorized access to issues list with certain configuration (JT-46159)	High	2018.1.40066	Not applicable
YouTrack	Custom fields allowed privilege escalation for guest user account (JT-46115)	Medium	2018.1.40025	Not applicable
YouTrack	Issue linking permission bypassing was available via "Create issue linked as..." (JT-25321)	Medium	2017.4.39533	Not applicable
YouTrack	Unauthorized access to issue content was possible even if guest user access was restricted in the bundle installer (JT-45284)	Low	2017.4.39083	Not applicable
YouTrack	Activity records for private fields were available to users with read-only permissions (JT-45282)	Medium	2017.4.39083	Not applicable