



National Cyber Emergency Response Team

Government of Pakistan



NCA-21.211026 – National CERT Advisory

PingCAP Unauthorized Access and Customer Data Exposure

PingCAP, the company behind TiDB and TiDB Cloud, has confirmed unauthorized access to internal cloud resources, theft of customer-related information and exposure of source code. According to its incident report dated 19 October 2026, stolen service-account credentials were used to access certain systems between 9 September and 7 October 2026. Its Japanese-language disclosure indicates that personal information relating to up to approximately 50,000 individuals in Japan may have been compromised.

Organizations using PingCAP services should prioritize API-key rotation, retrospective log review and confirmation of customer-specific exposure. PingCAP has not confirmed unauthorized access to customer TiDB Cloud databases or compromise of data stored in those databases. Exposure varies by customer and the investigation remains ongoing. Threat intelligence update: 21 October 2026.

DOCUMENT SUMMARY

Field	Details
Advisory ID	To be assigned
Threat Type	Unauthorized access / Customer information exposure / Source-code theft
Severity	High (Customer action required)
Attack Vector	Misuse of stolen service-account credentials to access internal cloud resources
Authentication Required	Valid service-account credentials were used
User Interaction	Not specified in the incident disclosure
Risk Rating	High (Information exposure and potential secondary credential misuse)
Scope & Applicability	Government, CII, financial institutions and other organizations using PingCAP services or TiDB Cloud; customer-specific impact remains under investigation

IMPACT ANALYSIS

Confirmed exposure and potential secondary risks include:

- User information:** Usernames, email addresses, and organization and project associations.
- Operational metadata:** SQL editor text, errors and some organization, project and cluster identifiers.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



3. **Commercial information:** Customer contacts, contracts, orders, pricing, payment terms and billing configurations.
4. **Credential-related records:** Encrypted API-key-related values were exported; exposure of usable private credentials has not been confirmed.
5. **Source code:** PingCAP confirmed that the unauthorized party obtained source code.
6. **Potential secondary risks:** Credential misuse, spear-phishing, vendor impersonation and unauthorized access attempts using exposed technical information.
7. **Customer database contents:** No evidence was identified of data stored in TiDB being affected. This does not establish that every customer or information category was exposed.

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Internal cloud-resource compromise and information exposure
Threat Status	Discovered 7 October 2026; known access paths blocked by 14 October; investigation ongoing as of 19 October
Initial Access	Stolen service-account credentials; initial unauthorized access dated 9 September 2026
Target Scope	PingCAP internal systems and associated customer information
Attack Complexity	Not disclosed
Privileges Required	Compromised service-account permissions; excessive cross-project permissions were subsequently removed
Affected Systems	Certain PingCAP internal cloud resources; customer TiDB Cloud database compromise has not been confirmed
Technical Disclosure	Four vendor-side vulnerabilities fixed; CVE identifiers, CVSS scores and affected software versions not disclosed

INDICATORS OF EXPOSURE / TARGETING

The incident disclosure reviewed does not provide confirmed attacker IP addresses, domains, file hashes or other attributable indicators of compromise. Conduct behavior-based hunting and investigate:

1. Unexpected creation, modification or deletion of API keys.
2. Unfamiliar source IP addresses, anomalous logins or unauthorized member invitations.
3. Unexpected privileged-role assignments or organization configuration changes.
4. Suspicious SQL statements, bulk queries or unauthorized exports.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



5. Abnormal cloud-storage reads, large downloads or anomalous service-account activity.
6. Messages impersonating PingCAP personnel, especially requests for credentials or account verification.
7. Unexpected execution of Data Import/Export or Backup tasks pointing to unauthorized third-party S3 buckets or external cloud storage endpoints.
8. Anomalous API calls executing query history exports or fetching stored SQL editor state files containing hardcoded credentials or sensitive customer PII.

REMEDIATION ACTIONS

1. Immediate Customer Security Measures

Action Category	Specific Actions
API-Key Rotation	Replace active TiDB Cloud management API keys; update applications and CI/CD integrations, test functionality and revoke superseded keys. Review Data Service API keys separately.
Retrospective Log Review	Review console, database, SSO and connected-cloud logs from 9 September 2026 onward; examine earlier activity where evidence permits.
Access Governance	Audit members, privileged accounts, project roles, integrations and machine identities. Remove unnecessary access; apply least privilege and MFA or SSO where supported.
Phishing Defences	Alert administrators, developers, finance and support teams. Independently verify messages claiming to originate from PingCAP.
Sensitive Information Review	Check SQL editor history, errors, support tickets and code for credentials, personal information or sensitive business data; revoke suspected exposed secrets.
Monitoring and Escalation	Enable appropriate audit logging, preserve evidence, contact PingCAP for customer-specific impact and activate incident response if unauthorized activity is found.
Database & Application Credential Rotation	In addition to TiDB Cloud Management API keys, immediately rotate all database user passwords, TLS/SSL certificates, and connected cloud integration tokens (e.g., AWS S3, GCP Bucket, or Azure Blob storage credentials used for TiDB backups/S3 imports) that were saved or referenced in TiDB Cloud consoles or SQL editor histories.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



2. Vendor Remediation Timeline

PingCAP reported the following containment and remediation measures:

Date	Response Area	Vendor-Reported Measures
7 October 2026	Initial containment	Revocation and disabling of affected credentials began after discovery.
10 October 2026	Access hardening	Additional compromised credentials deleted; excessive cross-project permissions removed; cloud-storage access logging enhanced.
12–13 October 2026	External assessment	An external incident response organization identified four security vulnerabilities.
14 October 2026	Containment and fixes	All identified compromised credentials invalidated; known unauthorized access paths blocked; all four vulnerabilities fixed and successfully retested by an independent external team.
19 October 2026	Ongoing investigation	Customer-specific exposure, possible earlier exploitation, additional credentials and remaining findings continued to be investigated.

Remediation Clarification

1. The confirmed initial access mechanism was misuse of stolen service-account credentials; this is not a confirmed TiDB database-engine vulnerability requiring a universal customer patch.
2. PingCAP has not publicly documented technical root causes or customer-deployable patches for the four vulnerabilities it fixed.
3. Self-managed TiDB operators should continue applying applicable official security updates. A database-engine upgrade alone should not be treated as remediation for this incident.
4. Vendor-reported containment measures do not independently certify that every possible consequence of the intrusion has been eliminated.

3. Patch and Technical Disclosure Status

Technical Item	Disclosed Status	Customer Implication
Vendor vulnerabilities	Four reported fixed by 14 October 2026; independent retesting successful	Continue following vendor updates
CVE / CVSS / Versions	Not disclosed in the incident report	No specific CVE or affected version range established
Customer patch package	No publicly documented incident-specific package identified	Do not rely on an engine upgrade alone
API-key rotation	Explicitly recommended in the Japanese notice	Replace and revoke keys; validate integrations

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

4. Logging and Operational Controls

Control Area	Specific Actions
Console Audit Logging	Enable logging where required. Console audit logging is disabled by default and retains records for 90 days.
Historical Evidence	Promptly export existing relevant records. Enabling logging now cannot recover activity that was never logged.
Database Audit Logging	Configure separately from console logging. Availability depends on TiDB Cloud product, supported version and configuration.
Integration Validation	After key rotation, verify applications and automation use replacement keys and superseded keys are revoked.
Vendor Coordination	Obtain customer-specific exposure confirmation and track further official incident updates.

"Note on Audit Logs Export: TiDB Cloud Console Audit Logging is disabled by default and caps log retention at 90 days. Organizations should immediately export all available historical audit logs from 9 September 2026 onwards to external SIEM or immutable cloud storage before the logs roll over and are permanently lost."

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Credential Protection	Rotate management API keys and other potentially exposed secrets.
Evidence Preservation	Export available logs promptly before retention periods expire.
Threat Hunting	Review suspicious identity, API, database and cloud-storage activity.
Access Review	Remove excessive privileges and unused accounts or integrations.
Exposure Assessment	Review SQL history and support records for sensitive content.
Staff Awareness	Warn relevant teams about targeted phishing and impersonation.
Incident Escalation	Confirm impact with PingCAP and escalate suspicious activity.



National Cyber Emergency Response Team

Government of Pakistan



PKCERT

MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Review CreateAPIKey, EditAPIKey and DeleteAPIKey events for unexpected changes.
2	Review LoginOrganization events for anomalous logins and unfamiliar source IP addresses.
3	Review InviteUserToOrganization and UpdateUserRoleInOrganization events for unauthorized access changes.
4	Correlate operator identity, source IP, timestamp and operation outcome across available audit records.
5	Investigate suspicious SQL statements, unexpected bulk queries and unauthorized exports.
6	Monitor abnormal storage reads, large downloads and service-account activity in connected cloud environments.
7	Preserve console, database, SSO and cloud logs; prioritize activity from 9 September 2026 onward.
8	Monitor messages impersonating PingCAP or using exposed organizational, commercial or technical details.
9	Set up automated alerts for Update Organization Security Settings and Create Service Account events to detect any persistence mechanisms established by unauthorized actors.

DISASTER RECOVERY & INCIDENT RESPONSE REQUIREMENTS

Phase	Requirement Area	Actions / Controls
1	Incident Identification	Validate suspicious activity using available logs; request customer-specific exposure information from PingCAP.
2	Immediate Containment	Revoke compromised or suspected exposed keys; remove unauthorized access and excessive permissions.
3	Evidence Preservation	Preserve relevant audit records, SQL history, support interactions and suspicious messages.
4	Secure Recovery	Replace affected credentials, update dependent integrations and verify authorized operation.
5	Post-Incident Actions	Assess downstream disclosure risks, strengthen access and logging controls, and complete reporting through established procedures.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



STRATEGIC PROTECTIVE MEASURES (CII & HIGH-VALUE TARGETS)

1. Maintain an inventory of TiDB Cloud organizations, projects, accounts, API keys and connected integrations.
2. Apply least-privilege access to human and machine identities, with periodic membership and role reviews.
3. Use MFA or enterprise SSO where supported and strengthen verification of vendor communications.
4. Maintain appropriate console, database and connected-cloud audit logging with timely evidence export.
5. Keep credentials out of SQL text, support tickets and code; review suspected exposure and rotate affected secrets.

INCIDENT REPORTING

Organizations identifying related unauthorized access, credential misuse or customer information exposure should activate their incident-response procedures, contact PingCAP for impact confirmation and report relevant incidents to National CERT Pakistan:

- **Incident Reporting Portal:** <https://pkcert.gov.pk/report-incident/>
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Rotate TiDB Cloud management API keys and revoke superseded credentials.
2	Review Data Service API keys and other secrets where exposure is suspected.
3	Preserve and review available logs from 9 September 2026 onward.
4	Audit privileged users, organization memberships, machine identities and integrations.
5	Assess SQL history, errors and support records for sensitive content.
6	Alert relevant staff to targeted phishing and PingCAP impersonation.
7	Enable appropriate audit logging and investigate unusual access or data transfers.
8	Obtain customer-specific exposure confirmation and escalate confirmed unauthorized activity.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk