INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-12 07:03 UTC

# ServiceNow tells customers a bug left some of their data exposed to the internet

DATA BREACH | HIGH | CVSS 7.5

| | |
|---|---|
| SCC Item ID | SCC-DBR-2026-0163 |
| Type | Data Breach |
| Severity | HIGH |
| CVSS Base Score | 7.5 |
| Affected Products | ServiceNow (enterprise platform, specific versions not confirmed in available sources) |
| Published | 1 day ago |
| Discovery Source | Serper |

## Executive Summary

ServiceNow disclosed that a software bug exposed enterprise customer data to the internet, with affected customers notified that their data was accessed. ServiceNow is deeply embedded in enterprise operations, handling IT service management, HR workflows, and operational processes, meaning exposed data may include sensitive internal records, employee information, or operational data depending on each customer's configuration. The full scope of affected customers, data types, and exposure duration remains unconfirmed; organizations using ServiceNow should treat this as an active data exposure event until ServiceNow provides definitive remediation guidance.

## Technical Analysis

ServiceNow disclosed a software bug classified under CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) that caused customer data to be inadvertently exposed to the internet. The exposure maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application). No CVE has been assigned; no NVD or CISA KEV entry exists as of 2026-06-10. A base severity rating of high (7.5) has been assigned editorially and does not derive from NVD vector scoring or CVSS framework; CVSS scoring does not directly apply to unpatched disclosures without CVE assignment. No vendor CVSS vector is available. Specific affected versions, the precise bug class, the data categories exposed, the number of affected tenants, and the exposure window have not been confirmed in available sources. Discovery source is TechCrunch (2026-06-10), a T2 source; no authoritative vendor advisory URL has been confirmed. No threat actor attribution has been established. Patch or mitigation details are not yet available from confirmed sources.

## Action Checklist

1. Step 1: Containment. Contact your ServiceNow account representative or support portal immediately to determine whether your tenant is among those notified as affected; do not wait for passive notification. Until ServiceNow confirms your tenant is unaffected, treat any sensitive data stored in your instance as potentially exposed. Review internet-facing ServiceNow integrations and confirm WAF or access controls are enforced on all external-facing endpoints (CIS 4.4, CIS 4.5).
2. Step 2: Detection. Review ServiceNow platform audit logs and access logs for anomalous or unauthorized access to records, particularly during the period prior to June 10, 2026. Query for access events originating from unexpected IP ranges or unauthenticated sessions against data tables containing employee, operational, or IT service records. Enable or verify that audit logging is active across your ServiceNow instance per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOC patterns or specific event IDs are available from current sources.
3. Step 3: Eradication. Apply any patch or configuration remediation issued by ServiceNow as soon as it is released through the official ServiceNow support portal. No specific patch ID or version upgrade path is confirmed in available sources at analysis time; monitor ServiceNow's official advisory channel. Enforce least-privilege access controls on all ServiceNow data tables (NIST AC-6, CIS 3.3) and review API key and integration credential permissions (D3-CRO: Credential Rotation; D3-CH: Credential Hardening).
4. Step 4: Recovery. After applying ServiceNow's remediation, validate that data exposure is no longer reproducible by conducting access testing against previously exposed endpoints. Review access logs post-remediation to confirm no continued unauthorized access. Rotate credentials and API tokens for any integrations that had access to affected data (D3-CRO). Verify audit logging captures post-fix access events per NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Conduct a review of data classification and access control configurations within your ServiceNow instance; confirm that sensitive data tables are not unintentionally exposed through public-facing portals or APIs. Map any confirmed data exposure to applicable regulatory notification obligations. Evaluate whether your ServiceNow configuration aligns with NIST AC-3 (Access Enforcement) and AC-4 (Information Flow Enforcement). Document lessons learned and update your third-party SaaS risk assessment process per NIST AC-20 (Use of External Systems).

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate to legal, privacy counsel, and executive leadership immediately if ServiceNow confirms your tenant was among those notified as affected and audit logs show access to tables containing PII, PHI, HR records, or regulated data — confirmed data access triggers breach notification assessment obligations under GDPR Article 33 (72-hour notification window), HIPAA §164.400, or applicable state statutes, and the exposure window duration is currently unconfirmed. |

| | |
|---|---|
| **Recovery Notes** | After ServiceNow releases and you apply the official remediation, conduct unauthenticated API and portal access testing against all externally reachable endpoints to confirm the exposure path is closed before resuming normal operations. Monitor the ServiceNow `syslog_transaction` and `sys_audit` tables daily for a minimum of 14 days post-remediation for any resumed anomalous access patterns from external IP ranges, particularly against sensitive data tables (`sys_user`, `hr_case`, `incident`, `sc_request`). Maintain forensic log exports from the exposure window in cold storage for at least 12 months to support any regulatory inquiry, legal hold, or downstream customer notification process. |
| **Forensic Artifacts** | ServiceNow `syslog_transaction` table: records all inbound API and portal transactions with caller IP, HTTP method, endpoint URI, authenticated user (or null for unauthenticated), and timestamp — primary artifact for reconstructing unauthorized access during the exposure window \| ServiceNow `sys_audit` table: records field-level read and write events on audited tables, enabling identification of which specific records and data fields were accessed by anomalous sessions \| ServiceNow System Log > All (`syslog` table): application-level error and access log capturing session establishment events, authentication failures, and platform errors that may reveal the mechanism of the exposure bug \| MID Server application logs (if self-hosted): located at `/agent/logs/agent0.log`, these record all integration transactions between the ServiceNow platform and internal enterprise systems and may show lateral data access triggered by compromised integration credentials \| Network perimeter/WAF logs for the ServiceNow tenant domain (e.g., `.service-now.com`): external-facing logs showing source IPs, request volumes, and URI patterns against ServiceNow endpoints during the exposure window, enabling identification of systematic enumeration or scraping activity against exposed data tables |

### Per-Action IR Details

**Step 1: Containment — Contact your ServiceNow account representative or support portal immediately to determine whether your tenant is among those notified as affected; do not wait for passive notification. Until ServiceNow confirms your tenant is unaffected, treat any sensitive data stored in your instance as potentially exposed. Review internet-facing ServiceNow integrations and confirm WAF or access controls are enforced on all external-facing endpoints (CIS 4.4, CIS 4.5).**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy

**Controls:** CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), NIST AC-4 (Information Flow Enforcement)

**Compensating:** Without a WAF appliance, use iptables or Windows Firewall to restrict inbound access to ServiceNow integration endpoints (e.g., MID Server ports, REST API listeners) to known corporate egress IPs only. Run `ss -tlnp` (Linux) or `netstat -ano` (Windows) on any self-hosted MID Servers to enumerate exposed ports. Block unauthenticated external access to ServiceNow's public-facing portal paths (/sp, /esc, /api/*) at the perimeter firewall or reverse proxy (nginx/Apache) using ACL rules.

**Evidence:** Before restricting access or modifying firewall rules, capture the current live network state: run `netstat -ano` or `Get-NetTCPConnection` on any self-hosted MID Servers and export active sessions to a timestamped file. Screenshot or export the current WAF/firewall rule set to document the pre-change baseline. If ServiceNow audit logs are accessible now, pull and preserve a snapshot of access events from the past 90 days before any configuration change could trigger log rotation or overwrite.

**Step 2: Detection — Review ServiceNow platform audit logs and access logs for anomalous or unauthorized access to records, particularly during the period prior to June 10, 2026. Query for access events originating from unexpected IP ranges or unauthenticated sessions against data tables containing employee, operational, or IT service records. Enable or verify that audit logging is active across your ServiceNow**

**instance per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOC patterns or specific event IDs are available from current sources.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, export ServiceNow audit logs (navigate to System Log > All in the ServiceNow UI, or query the `sys_audit` and `syslog` tables via REST API using: `GET /api/now/table/sys_audit?sysparm_query=tablename=TABLENAME^sys_created_onBETWEENjavascript:gs.dateGenerate('STARTDATE')@javascript:gs.dateGenerate('ENDDATE')`) and pipe results to a local CSV. Use Python or PowerShell to parse for access events where `source_ip` falls outside known corporate CIDR ranges, or where `user` is null/anonymous. Flag any reads against sensitive tables such as `sys_user`, `hr_case`, `task`, or `incident` originating from external IPs.

**Evidence:** Volatile evidence to capture before enabling or modifying logging settings (which may reset counters or trigger log rotation): export the current contents of the ServiceNow `syslog_transaction` table (records all inbound REST/SOAP transactions including caller IP, endpoint URI, and HTTP method) and the `sys_audit` table filtered to the suspected exposure window. Document any currently active sessions visible in System Diagnostics > Active Transactions before making changes. These tables are the primary forensic record of whether unauthenticated or anomalous access actually reached data records.

**Step 3: Eradication — Apply any patch or configuration remediation issued by ServiceNow as soon as it is released through the official ServiceNow support portal. No specific patch ID or version upgrade path is confirmed in available sources at analysis time; monitor ServiceNow's official advisory channel. Enforce least-privilege access controls on all ServiceNow data tables (NIST AC-6, CIS 3.3) and review API key and integration credential permissions (D3-CRO: Credential Rotation; D3-CH: Credential Hardening).**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST AC-6 (Least Privilege), CIS 3.3 (Configure Data Access Control Lists), NIST AC-2 (Account Management)

**Compensating:** Before applying the ServiceNow patch, export a full list of all active API keys and integration accounts via the `sys_auth_profile_exact` and `sys_user` tables (filter on `active=true` and `web_service_access_only=true`). Revoke any API credentials not tied to a documented integration. Use ServiceNow's built-in Access Control List (ACL) editor (Security > Access Control) to audit table-level read permissions and remove public or unauthenticated read access on sensitive tables (`sys_user`, `hr_case`, `incident`, `sc_request`). Document the ACL state before and after changes as your eradication evidence record.

**Evidence:** Volatile evidence to capture BEFORE applying any patch or revoking API credentials: snapshot all currently active ServiceNow sessions (System Diagnostics > Active Transactions) and export active integration credentials and their last-used timestamps from `sys_auth_profile_exact`. Pull the current ACL configuration from Security > Access Control and save to a dated export — this documents the pre-patch permission state that allowed the exposure and serves as evidence for root cause analysis. Credential rotation after this capture is safe.

**Step 4: Recovery — After applying ServiceNow's remediation, validate that data exposure is no longer reproducible by conducting access testing against previously exposed endpoints. Review access logs post-remediation to confirm no continued unauthorized access. Rotate credentials and API tokens for any integrations that had access to affected data (D3-CRO). Verify audit logging captures post-fix access events per NIST AU-6 (Audit Record Review, Analysis, and Reporting).**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-17 (Remote Access), CIS 5.2 (Use Unique Passwords)

**Compensating:** Use `curl` or Postman to replay unauthenticated GET requests against the ServiceNow REST API endpoints and public-facing portal paths (e.g., `/api/now/table/sys_user` without an Authorization header) post-patch and confirm HTTP 401 or 403 responses are returned. For API token rotation without an IAM platform, generate new OAuth credentials in ServiceNow (System OAuth > Application Registry), update all downstream integration configs, then revoke old tokens and document the rotation with timestamps. Monitor the `syslog_transaction` table daily for 14 days post-recovery for any resumed unauthorized access patterns.

**Evidence:** Before rotating credentials or conducting access validation testing, capture a post-patch snapshot of the `syslog_transaction` and `sys_audit` tables to establish a clean baseline timestamp. This timestamp anchors your 'exposure ended' claim for any regulatory notification. Record the exact patch version or configuration change applied, the date/time applied, and the identity of the admin who applied it — this constitutes the chain-of-custody record for the remediation action.

**Step 5: Post-Incident — Conduct a review of data classification and access control configurations within your ServiceNow instance; confirm that sensitive data tables are not unintentionally exposed through public-facing portals or APIs. Map any confirmed data exposure to applicable regulatory notification obligations. Evaluate whether your ServiceNow configuration aligns with NIST AC-3 (Access Enforcement) and AC-4 (Information Flow Enforcement). Document lessons learned and update your third-party SaaS risk assessment process per NIST AC-20 (Use of External Systems).**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity

**Controls:** NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), NIST AC-20 (Use Of External Systems), CIS 3.2 (Establish and Maintain a Data Inventory), NIST AU-11 (Audit Record Retention)

**Compensating:** Produce a ServiceNow data inventory by querying all tables with active records via the Schema Map (System Definition > Tables) and tagging those containing PII, HR, or operational data. Cross-reference each table against its ACL configuration to identify any residual public-read permissions. For regulatory mapping, use a simple spreadsheet to match confirmed exposed data fields (e.g., employee names, email addresses, ticket contents) against GDPR Article 33, HIPAA §164.400, or applicable state breach notification statutes — this mapping drives your notification timeline and scope.

**Evidence:** Retain the full set of forensic artifacts collected during the incident — ServiceNow `sys_audit` and `syslog_transaction` exports, pre- and post-patch ACL configuration snapshots, credential rotation records, and access validation test results — for a minimum of 12 months or as required by applicable regulatory retention obligations (NIST AU-11). These records constitute the evidentiary basis for any regulatory notification, legal hold, or future audit inquiry related to this exposure event.

## Detection Guidance

No confirmed IOCs, specific event IDs, or forensic indicators are available from current sources. Organizations should pull ServiceNow instance access logs and audit trail records for the period prior to June 10, 2026, querying for: access to sensitive data tables from IP addresses outside expected corporate or integration ranges; unauthenticated or anonymously attributed access events; bulk record reads or exports that lack corresponding authorized user activity; and API calls from unknown or dormant integration accounts. Enable full audit logging if not already active (NIST AU-2, AU-12; CIS 8.2). Use ServiceNow's native audit trail and security logging features. Cross-reference any suspicious access events against your identity and access management records. If ServiceNow issues a formal advisory with specific indicators or affected component details, update detection queries accordingly. Note: absence of suspicious log entries does not confirm you are unaffected if logging was not comprehensive during the exposure window.

## Framework Mappings

### MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

### NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

### OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

### HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

### SOC2-TSC

- **CC7.4** — Responds to identified security incidents

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| | https://techcrunch.com/2026/06/10/servicenow-tells-customers-a-bug-... | T2 |
| **ServiceNow tells customers a bug left some of their data exposed to ...** | https://www.reddit.com/r/servicenow/comments/1u24urt/techcrunch_ser... | T3 |

| Source | URL | Tier |
|---|---|---|
| **ServiceNow tells customers a bug left some of their data exposed to ...** | https://x.com/TechCrunch/status/2064712757887508861 | T3 |
| **ServiceNow tells customers a bug left some of their data exposed to ...** | https://www.linkedin.com/posts/techcrunch_servicenow-tells-customer... | T3 |
| **ServiceNow says bug exposed customer data online** | https://americanbazaaronline.com/2026/06/10/servicenow-says-bug-exp... | T3 |



Generated 2026-06-12 07:03 UTC by TJS Security Command Center