INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:24 UTC

# ServiceNow Unauthenticated API Flaw Actively Exploited, Customer Instance Data Exposed Across Enterprise Deployments

**DATA BREACH** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-DBR-2026-0155 |
| **Type** | Data Breach |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | ServiceNow, Australia platform release and older releases with certain configuration changes |
| **Published** | 2026-06-09T17:34:09 |
| **Discovery Source** | Rss |

## Executive Summary

Attackers exploited an unauthenticated REST API endpoint in ServiceNow to access sensitive customer instance data, including support tickets, employee records, credentials, and internal documentation, without requiring any login credentials. Organizations running ServiceNow on the Australia platform release or older releases with certain configuration changes are affected; ServiceNow applied a patch on June 5, 2026, and has opened support cases with affected customers. The business risk is significant: ServiceNow instances typically aggregate enterprise-wide operational data across IT workflows, meaning a single compromised instance can expose credentials and records usable for follow-on attacks.

## Technical Analysis

An unauthenticated REST API endpoint in ServiceNow allowed network-based access to sensitive customer instance data without authorization. The vulnerability is rooted in missing authentication controls on the API layer, mapped to CWE-306 (Missing Authentication for Critical Function), CWE-284 (Improper Access Control), and CWE-863 (Incorrect Authorization). No CVE identifier has been assigned or confirmed at time of writing. Affected scope is the ServiceNow Australia platform release and older releases with certain configuration changes. Attack surface is network-accessible with no authentication prerequisite (CVSS base 7.5, high severity). Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1552.001 (Credentials in Files), and T1078 (Valid Accounts). ServiceNow issued a patch on June 5, 2026, and has proactively contacted affected customers. No CVE, EPSS score, or CISA KEV entry is confirmed. Source quality score is 0.64;

BleepingComputer and ServiceNow release notes and security notables pages are listed as corroborating sources. Human verification of source URLs is recommended before citing them in formal reporting.

## Action Checklist

1. Step 1: Containment. Identify all ServiceNow instances running the Australia platform release or older releases with configuration changes affecting API authentication. Restrict inbound access to the REST API endpoint to known IP ranges or VPN egress points at the network perimeter immediately, with completion target within 4 hours. If internet-facing instances cannot be restricted within that window, escalate to ServiceNow support to request temporary endpoint deactivation pending patching. Reference: NIST AC-4 (Information Flow Enforcement), enforce approved authorizations for controlling information flow between connected systems.
2. Step 2: Detection. Review ServiceNow access logs and REST API request logs for unauthenticated GET or POST requests to sensitive API endpoints, particularly requests that returned HTTP 200 without a valid session token or user context. Look for high-volume or off-hours queries against ticket, employee record, or credential store tables. Correlate with source IPs for patterns consistent with automated scraping (sequential record access, uniform timing intervals). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), review audit records for indications of inappropriate activity.
3. Step 3: Eradication. Apply the ServiceNow patch issued June 5, 2026, to all affected instances. Confirm patch application against ServiceNow's Australia security notables page. For instances not yet patched, enforce authentication controls on the affected REST API endpoint via ServiceNow access control rules (ACLs) as an interim mitigation. Disable or restrict the specific endpoint if ACL enforcement cannot be confirmed. Reference: CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management), apply updates on a monthly or more frequent basis.
4. Step 4: Recovery. After patching, validate that the previously affected API endpoint now returns HTTP 401 or 403 for unauthenticated requests. Run a controlled test from an unauthenticated network context to confirm authentication enforcement. Monitor ServiceNow logs for 7 to 14 days post-patch for residual unauthorized access attempts. Review any support cases opened by ServiceNow on your behalf and confirm remediation steps are documented. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), analyze audit records at defined frequency for indications of anomalous activity post-remediation.
5. Step 5: Post-Incident. Audit all data exposed through the affected endpoint: identify what employee records, credentials, tickets, and documentation were accessible and assess downstream risk. Rotate any credentials confirmed or suspected to have been exposed (reference D3-CRO: Credential Rotation). Review ServiceNow ACL configurations across all instances to identify any other endpoints with missing or insufficient authentication controls. Establish a recurring review cycle for API authentication posture. Reference: NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege), enforce approved authorizations and apply least-privilege principles to API access. Reference D3-UAP (User Account Permissions), restrict account access to resources. Flag potential regulatory exposure to legal and compliance teams before disclosing publicly.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CISO, legal counsel, and privacy officer immediately if forensic log review confirms unauthenticated HTTP 200 responses against sys_user, incident, or discovery_credentials tables — indicating actual data exfiltration of PII, employee records, or credentials that may trigger GDPR Article 33, state breach notification laws, or contractual disclosure obligations to affected customers. |
| **Recovery Notes** | After the June 5, 2026 patch is applied and validated via unauthenticated curl testing, monitor ServiceNow syslog_transaction daily for 14 days for any null-user HTTP 200 responses against REST endpoints, which would indicate either a missed instance or a patch regression. Verify that all ServiceNow support cases opened on your behalf by ServiceNow's customer success team are closed with documented remediation confirmation — retain these as audit evidence. Do not restore any previously restricted network access paths until the 14-day monitoring window completes clean. |
| **Forensic Artifacts** | ServiceNow syslog_transaction table records: rows with null/empty user field, HTTP method GET or POST, response code 200, and URI matching /api/now/table/* — these are the direct evidence of unauthenticated API exploitation against this specific vulnerability \| ServiceNow sys_audit table records: read-operation audit entries on the incident, sys_user, sys_user_group, and discovery_credentials tables attributed to a null or guest user context during the exploitation window \| Reverse proxy or load balancer HTTP access logs (nginx access.log, Apache access.log, AWS ALB access logs, or Cloudflare logs): entries showing requests to the ServiceNow REST API path without an Authorization or X-UserToken header returning HTTP 200, including source IP, User-Agent, and bytes-transferred fields that reveal scraping tool signatures and volume of data exfiltrated \| ServiceNow sys_security_acl table snapshot: ACL configuration records for affected REST endpoint tables at the time of exploitation — documents the misconfiguration or missing authentication control that permitted unauthenticated access and serves as the baseline for post-incident hardening comparison \| Network flow or firewall session logs (NetFlow, IPFIX, or firewall connection tables): external IP-to-ServiceNow-instance TCP/443 sessions with high byte counts or high request frequency during the exploitation window — sequential record-access patterns with uniform inter-request timing intervals are indicators of automated scraping of ServiceNow table data |

### Per-Action IR Details

**Step 1: Containment — Identify all ServiceNow instances running the Australia platform release or older releases with configuration changes affecting API authentication. Restrict inbound access to the REST API endpoint to known IP ranges or VPN egress points at the network perimeter immediately. If internet-facing instances cannot be restricted within hours, work with ServiceNow support to take the affected endpoint offline pending patching. Reference: NIST AC-4 (Information Flow Enforcement) — enforce approved authorizations for controlling information flow between connected systems.**

**NIST Phase:** Containment

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

**Controls:** NIST AC-4 (Information Flow Enforcement)

**Compensating:** For teams without a WAF or next-gen firewall: use iptables or Windows Firewall with Advanced Security to create an allowlist rule permitting only corporate egress IPs to reach the ServiceNow instance URL on TCP/443. On Linux perimeter hosts: `iptables -A INPUT -p tcp --dport 443 -s -j ACCEPT && iptables -A INPUT -p tcp --dport 443 -j DROP`. Document every IP range added. If the instance is cloud-hosted (ServiceNow SaaS), raise an emergency support ticket requesting IP allowlisting at the platform level — this is a documented ServiceNow support capability.

**Evidence:** Before restricting access, capture a full export of ServiceNow REST API transaction logs from the sys_log_email, sys_audit, and syslog_transaction tables covering the 30 days prior to June 5, 2026 (patch date). Preserve raw HTTP access logs from any reverse proxy or load balancer fronting the ServiceNow instance, specifically retaining entries with no Authorization header and HTTP 200 response codes against REST endpoints (e.g., /api/now/table/). Snapshot firewall flow logs or NetFlow data showing external IP-to-instance connections on TCP/443 for the same window.

**Step 2: Detection — Review ServiceNow access logs and REST API request logs for unauthenticated GET or POST requests to sensitive API endpoints, particularly requests that returned HTTP 200 without a valid session token or user context. Look for high-volume or off-hours queries against ticket, employee record, or credential store tables. Correlate with source IPs for patterns consistent with automated scraping (sequential record access, uniform timing intervals). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) — review audit records for indications of inappropriate activity.**

**NIST Phase:** Detection Analysis

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

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

**Compensating:** Without a SIEM, query ServiceNow's syslog_transaction table directly via the platform UI or a privileged REST call: filter on `response_time` records where `user` is empty or null and `status` = 200, targeting URI patterns matching `/api/now/table/incident`, `/api/now/table/sys_user`, or `/api/now/table/x_*` (custom credential stores). Export results to CSV and use `sort | uniq -c | sort -rn` in bash to surface high-frequency source IPs. Cross-reference IPs against free threat intel (e.g., AbuseIPDB bulk lookup via their free API) to flag known scanner or VPN exit node addresses.

**Evidence:** Preserve the ServiceNow syslog_transaction table records (includes URI, HTTP method, response code, session ID, and remote IP) for the full exploitation window. Capture sys_audit table entries showing read operations on the incident, sys_user, sys_user_group, and any credential-storing tables (e.g., discovery_credentials) with a null or guest user context. Retain any WAF or CDN access logs (Cloudflare, Akamai, AWS CloudFront) showing unauthenticated API calls — these often capture User-Agent strings that identify the scraping tool used.

**Step 3: Eradication — Apply the ServiceNow patch issued June 5, 2026, to all affected instances. Confirm patch application against ServiceNow's Australia security notables page. For instances not yet patched, enforce authentication controls on the affected REST API endpoint via ServiceNow access control rules (ACLs) as an interim mitigation. Disable or restrict the specific endpoint if ACL enforcement cannot be confirmed. Reference: NIST SI-4 (no mapped control — SI family not included in the provided knowledge base extract); CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) — apply updates on a monthly or more frequent basis.**

**NIST Phase:** Eradication

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

**Controls:** CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

**Compensating:** For teams unable to patch immediately: navigate to ServiceNow's Access Control (ACL) table (sys_security_acl) and create a deny ACL on the affected REST endpoint table scoped to the `nobody` role with no conditions — this blocks unauthenticated callers. Verify enforcement by issuing a curl test from a machine with no active ServiceNow session: `curl -v -X GET 'https://.service-now.com/api/now/table/?sysparm_limit=1'` — a correctly configured ACL will return HTTP 401. Document the ACL sys_id and the tester's IP for the incident record.

**Evidence:** Before applying the patch, capture a full export of ServiceNow's sys_update_set table to document the pre-patch ACL and configuration baseline. Record the current platform version from the sys_properties table (glide.buildname or glide.build.date properties) to confirm the instance was running the Australia release or an affected older release. Preserve any custom ACL overrides on REST endpoint tables that may have weakened default authentication — these are eradication targets and must be documented before the patch overwrites platform defaults.

**Step 4: Recovery — After patching, validate that the previously affected API endpoint now returns HTTP 401 or 403 for unauthenticated requests. Run a controlled test from an unauthenticated network context to confirm authentication enforcement. Monitor ServiceNow logs for 7 to 14 days post-patch for residual unauthorized access attempts. Review any support cases opened by ServiceNow on your behalf and confirm remediation steps are documented. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — analyze audit records at defined frequency for indications of anomalous activity post-remediation.**

**NIST Phase:** Recovery

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

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting)

**Compensating:** Without automated monitoring, configure a daily cron job or scheduled task running: `curl -s -o /dev/null -w '%{http_code}' -X GET 'https://.service-now.com/api/now/table/?sysparm_limit=1'` and alert on any response other than 401 or 403. Simultaneously, set a daily export of the ServiceNow syslog_transaction table filtered for null-user 200-response entries to a shared mailbox — any entries appearing post-patch indicate either patch failure or a second unpatched instance. Retain these test results as documented evidence of remediation verification.

**Evidence:** Capture the HTTP response headers and body from the post-patch unauthenticated curl test — the 401/403 response with a WWW-Authenticate header is your forensic proof of remediation. Preserve the ServiceNow support case number and any remediation confirmation emails from ServiceNow's customer success team as chain-of-custody records. Export the sys_properties and sys_update_set tables post-patch to document the new platform build version as the authoritative baseline going forward.

**Step 5: Post-Incident — Audit all data exposed through the affected endpoint: identify what employee records, credentials, tickets, and documentation were accessible and assess downstream risk. Rotate any credentials confirmed or suspected to have been exposed (reference D3-CRO: Credential Rotation). Review ServiceNow ACL configurations across all instances to identify any other endpoints with missing or insufficient authentication controls. Establish a recurring review cycle for API authentication posture. Reference: NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) — enforce approved authorizations and apply least-privilege principles to API access. Reference D3-UAP (User Account Permissions) — restrict account access to resources. Flag potential regulatory exposure to legal and compliance teams before disclosing publicly.**

**NIST Phase:** Post Incident

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

**Controls:** NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** For credential rotation without an enterprise PAM tool: export the ServiceNow sys_user table to identify all accounts whose records were readable via the affected endpoint, then force password resets via Active Directory (`Set-ADUser -ChangePasswordAtLogon $true`) or identity provider bulk reset. For API/service account credentials stored in ServiceNow's discovery_credentials or external credential tables, manually rotate each and update referencing configuration items. To audit remaining ACL gaps, run a ServiceNow background script querying sys_security_acl for records with `operation=read` and an empty or wildcard role field across all REST-accessible tables — export and triage by data sensitivity.

**Evidence:** Compile the full list of ServiceNow table records accessed during the exploitation window from syslog_transaction (filter: null user, HTTP 200, REST API URI pattern) — this is your data exposure manifest for regulatory notification assessment. Preserve sys_user and sys_user_group table exports from the exposure window to document exactly which employee records were readable. Retain discovery_credentials and any other credential-storing table exports to enumerate secret material at risk. Archive all of the above with chain-of-custody notes in the incident record before initiating any credential rotation or regulatory disclosure.

## Detection Guidance

Query ServiceNow REST API transaction logs for requests that completed successfully (HTTP 200) against sensitive table endpoints (sc_req_item, sys_user, incident, kb_knowledge, sn_hr_core_case, or equivalent) where no authenticated session token or user sys_id is present in the request context. Flag source IPs making more than a threshold number of API calls within a short window without authentication. Look for sequential record retrieval patterns suggesting automated enumeration. In SIEM, correlate ServiceNow API logs with network flow data to identify external source IPs accessing the API outside business hours or from unfamiliar geographies. If ServiceNow's MID Server or integration logs are available, review for unexpected outbound data transfers. Reference: NIST AU-3 (Content of Audit Records), ensure audit records capture what event occurred, when, where, source and destination. Reference D3-LAM (Local Account Monitoring), analyze accounts to detect unauthorized activity. Specific ServiceNow log table names and API endpoint paths should be validated against your instance configuration and ServiceNow's incident advisory.

## Framework Mappings

### MITRE-ATTACK

- **T1552.001** — Credentials In Files
- **T1530** — Data from Cloud Storage
- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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

### OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

### CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.8** — Define and Maintain Role-Based Access Control
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

**SOC2-TSC**

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

**HIPAA-SECURITY**

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

**ISO-27001-2022**

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

**NIST-CSF-2**

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1552.001 | Credentials In Files | Credential-Access |
| T1530 | Data from Cloud Storage | Collection |
| T1213 | Data from Information Repositories | Collection |
| T1078 | Valid Accounts | Defense-Evasion |
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/servicenow-discloses... | T3 |
| **Australia security and notable fixes - ServiceNow** | https://www.servicenow.com/docs/r/release-notes/australia-security-... | T3 |
| **Australia release notes - ServiceNow** | https://www.servicenow.com/docs/r/release-notes/family-release-note... | T3 |
| **Part 6: Security, GRC, Early Release Strategy, Rea... - ServiceNow** | https://www.servicenow.com/community/upgrades-and-patching-forum/pa.. . | T3 |

| Source | URL | Tier |
| --- | --- | --- |
| **How the ServiceNow Australia Release Modernises SecOps** | https://www.devoteam.com/expert-view/how-servicenow-australia-relea... | T3 |



Generated 2026-06-10 07:24 UTC by TJS Security Command Center