INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-14 06:43 UTC

ServiceNow Security Incident: Unauthenticated API Flaw Exposes Customer Data

DATA BREACH | **HIGH** | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0170
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ServiceNow platform (specific versions not confirmed in available data)
Published	2 days ago
Discovery Source	Serper

Executive Summary

ServiceNow disclosed a security incident in which an unauthenticated API vulnerability allowed attackers to access customer data without valid credentials. The flaw, reported on June 10, 2026, affected organizations running ServiceNow in production environments and was disclosed directly to impacted customers. The business risk includes exposure of sensitive enterprise data stored within ServiceNow instances, potential downstream regulatory liability, and reputational damage for organizations relying on the platform for IT service management and workflow automation.

Technical Analysis

ServiceNow disclosed an unauthenticated access vulnerability affecting an API endpoint on its platform. Attackers exploited this flaw to access customer data without authentication. The weakness maps to CWE-306 (Missing Authentication for Critical Function) and CWE-284 (Improper Access Control). MITRE ATT&CK techniques involved are T1190 (Exploit Public-Facing Application) and T1530 (Data from Cloud Storage). No CVE identifier has been confirmed in the available source data. Affected version range has not been specified in the raw data provided. CVSS base score is reported at 7.5 (High). EPSS score and CISA KEV status are not confirmed. ServiceNow notified affected customers directly. No vendor-confirmed patch identifier or specific remediation build number is available in the current source data. Organizations should monitor the official ServiceNow Security Response page for patch details and version-specific guidance.

Action Checklist

1. Step 1: Containment, Immediately audit all ServiceNow API endpoint configurations, focusing on public-facing or externally accessible APIs that do not require authentication. Disable or restrict unauthenticated API access where not operationally required. Apply network-layer controls (WAF rules, IP allowlisting) to limit inbound access to ServiceNow API endpoints. Reference NIST AC-4 (Information Flow Enforcement) to enforce approved data flow authorizations between ServiceNow and external systems, ensuring API calls are restricted to authenticated, authorized sources.
2. Step 2: Detection, Review ServiceNow audit logs and transaction logs for unauthenticated API calls, anomalous data retrieval requests, or access patterns from unexpected IP ranges during the June 2026 window and preceding weeks. Query for HTTP 200 responses to API endpoints without associated authenticated session tokens. Correlate with AU-6 (Audit Record Review, Analysis, and Reporting) procedures. Confirm whether your organization received a direct notification from ServiceNow identifying affected instances.
3. Step 3: Eradication, Apply any ServiceNow-issued patch or configuration remediation once confirmed through the official ServiceNow Security Response portal. Enforce authentication requirements on all API endpoints per CWE-306 remediation guidance. Review and harden all ACL (Access Control List) rules within your ServiceNow instance to align with CIS 3.3 (Configure Data Access Control Lists) and NIST AC-3 (Access Enforcement). Remove or disable any API integrations that do not require unauthenticated access.
4. Step 4: Recovery, After remediation, validate that all ServiceNow API endpoints require valid authentication before returning data. Re-run access control audits across the platform. Monitor ServiceNow logs for residual anomalous access attempts. Confirm with ServiceNow support that your instance is no longer in the affected population. Align ongoing monitoring with AU-6 and CIS 8.2 (Collect Audit Logs) to ensure continued visibility.
5. Step 5: Post-Incident, Conduct a formal review of API security controls across all enterprise SaaS platforms, not only ServiceNow. Map findings against NIST AC-17 (Remote Access) and AC-20 (Use of External Systems) to assess gaps in vendor-hosted access governance. Update third-party risk management procedures to require SaaS vendors to disclose API authentication standards. Document this incident as a control gap driver for CIS 6.1 (Establish an Access Granting Process) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

Detection Guidance

Query ServiceNow transaction logs (syslog, sys_log_email, or your SIEM pipeline ingesting ServiceNow audit events) for API calls that returned HTTP 200 status without an associated authenticated user session or valid OAuth/SAML token. Look for high-volume or automated GET requests to REST API or JSON/XML endpoints originating from external IP ranges, particularly during the June 2026 disclosure window. Flag requests accessing user_data, sys_user, or customer record tables without session authentication. Monitor service account and API integration account access logs for anomalous data volumes inconsistent with their defined function. If your SIEM has a ServiceNow connector, create a detection rule alerting on unauthenticated API responses returning data payloads above a defined byte threshold. Cross-reference source IPs against known threat intelligence feeds. No confirmed IOC values (IP addresses, hashes, domains) are available in the current source data.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1530** — Data from Cloud Storage

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
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
	https://www.bleepingcomputer.com/news/security/servicenow-discloses...	T3
ServiceNow discloses security incident exposing customer data	https://www.reddit.com/r/servicenow/comments/1u24177/servicenow_dis...	T3
ServiceNow tells customers a bug left some of their data exposed to ...	https://techcrunch.com/2026/06/10/servicenow-tells-customers-a-bug-...	T2
ServiceNow data breach: security issue gives attacker access	https://cybernews.com/security/servicenow-confirms-security-inciden...	T3
ServiceNow discloses security incident exposing customer data ...	https://x.com/rootedcon/status/2064675206694686991	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-14 06:43 UTC by TJS Security Command Center