INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

Telus Digital Confirms Data Breach, ShinyHunters Claims ~1 Petabyte Stolen

DATA BREACH | HIGH | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0021
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Telus Digital (Canadian BPO subsidiary of Telus Corporation), internal systems and customer/employee data repositories
Published	2026-03-13

Executive Summary

Telus Digital, a Canadian BPO subsidiary of Telus Corporation, confirmed a security breach after threat actor group ShinyHunters claimed to have exfiltrated approximately 1 petabyte of data, including employee PII, customer data held on behalf of Telus Digital clients, and internal business records. The full scope has not been confirmed by the company; an investigation is ongoing. Organizations that engage Telus Digital as a BPO or data processor face potential third-party data exposure risk and should assess their contractual breach notification obligations.

Technical Analysis

Telus Digital confirmed unauthorized access to internal systems; the breach vector has not been officially disclosed. ShinyHunters, a financially motivated threat actor group with a history of large-scale data theft and extortion (MITRE T1657: Financial Motivated Extortion), advertised approximately 1 petabyte of alleged data for sale on underground forums. Applicable CWEs based on available reporting: CWE-284 (Improper Access Control), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), CWE-522 (Insufficiently Protected Credentials). Mapped MITRE ATT&CK techniques: T1078 (Valid Accounts, potential credential compromise as initial access vector), T1530 (Data from Cloud Storage), T1041 (Exfiltration Over C2 Channel), T1657 (Financial Motivated Extortion). No CVE applies; this is a breach incident, not a disclosed software vulnerability. No patch action is applicable. Qualitative severity is high given data volume and PII involvement; CVSS does not apply to data breach incidents. Breach scope, affected client list, and confirmed exfiltration volume remain unverified pending investigation completion.

Action Checklist

1. Step 1, Vendor Assessment: Determine whether your organization shares data with Telus Digital as a BPO client or data processor; identify data categories and volumes involved.
2. Step 2, Contract Review: Review your data processing agreement with Telus Digital for breach notification timelines and obligations; escalate to legal if notification deadlines apply.
3. Step 3, Credential Audit: If your organization uses any shared authentication, SSO, or API integrations with Telus Digital systems, rotate credentials and revoke active sessions immediately (T1078).
4. Step 4, Stakeholder Notification: Notify affected internal teams (legal, compliance, privacy officer) and assess regulatory reporting obligations under applicable frameworks (PIPEDA, GDPR if EU data subjects involved).
5. Step 5, Third-Party Risk Review: Audit BPO and data processor relationships for access controls, data minimization practices, and contractual security requirements; update vendor risk assessments for Telus Digital pending breach scope confirmation.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to C-level and external IR firm immediately if your organization transmitted EU resident data to Telus Digital (GDPR mandatory 72-hour breach notification to DPA applies regardless of confirmation of actual access), or if Telus Digital held payment card data (PCI-DSS notification to card brands required within 30 days).
Recovery Notes	Post-containment: (1) Monitor Telus Digital's public statements and regulatory filings for final breach scope confirmation; update your affected data subject count and notification obligations as scope clarifies. (2) Conduct a post-incident review with legal, IT, and compliance to document lessons learned: did your vendor risk assessment process flag Telus Digital's access control weaknesses? If not, strengthen your SAQ/attestation requirements. (3) Implement a quarterly vendor security review cycle for all BPOs holding sensitive data, informed by NIST 800-53 SA-9 and CIS 6.x controls.
Forensic Artifacts	Windows Event Log 4624 (logon), 4625 (logon failure), 4647 (session initiated) — filtered for Telus Digital service accounts and integrations | /var/log/auth.log and /var/log/audit/audit.log (Linux/Unix) — SSH sessions, sudo usage, user authentication events tied to Telus Digital data access | API access logs and application audit logs — timestamps, originating IPs, and data categories for Telus Digital API calls and batch data transfers | Network flow data (NetFlow, sFlow, or firewall logs) — source/destination IPs, ports, and volume for traffic to Telus Digital infrastructure; baseline 90-day pattern for anomaly detection | Browser download history and email attachment logs — employee or service account downloads of large data sets potentially related to exfiltration or unauthorized copying

Per-Action IR Details

Step 1, Vendor Assessment: Determine whether your organization shares data with Telus Digital as a BPO client or data processor; identify data categories and volumes involved.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase) and §4.2 (Third-party risk)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 CA-8 (Continuous Monitoring), CIS 6.1 (Establish processes for secure onboarding/offboarding)

Compensating: Manually query your contracts management system (or spreadsheet if unavailable) for Telus Digital references. Cross-reference with procurement records, service account inventories, and API integration documentation. If no centralized registry exists, query IT for active Telus Digital DNS names, IP ranges, or service accounts using `nslookup`, `whois`, and network configuration reviews.

Evidence: Capture before assessment: (1) Service account audit logs from Active Directory or IAM system showing last login timestamps for any Telus Digital-related accounts; (2) network flow logs (NetFlow/sFlow) for the past 90 days filtered on Telus Digital IP ranges or domains to establish baseline data flow patterns; (3) data catalog or DLP tool logs showing data classification tags associated with Telus Digital destinations.

Step 2, Contract Review: Review your data processing agreement with Telus Digital for breach notification timelines and obligations; escalate to legal if notification deadlines apply.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation) and §3.1 (Detection and Analysis — notification requirements)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-6 (Incident Reporting), CIS 6.2 (Establish third-party security requirements)

Compensating: If legal holds the master DPA, request sections covering (a) breach notification timeline, (b) your right to audit Telus Digital post-breach, and (c) liability/indemnification clauses. Document the notification deadline in writing and set a calendar alert 2 business days before the deadline. If no DPA exists, this gap itself is a control finding — escalate immediately.

Evidence: Preserve before escalation: (1) Email thread showing when your organization was first notified of the Telus Digital breach (timestamps and sender); (2) copy of the active data processing agreement (execution date, amendment history) to establish contractual obligations; (3) records of any prior breach notifications from Telus Digital or security audit findings to establish pattern of disclosure.

Step 3, Credential Audit: If your organization uses any shared authentication, SSO, or API integrations with Telus Digital systems, rotate credentials and revoke active sessions immediately (T1078).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment) and §3.2.4 (Eradication — credential management)

Controls: NIST 800-53 IA-4 (Identifier Management), NIST 800-53 AC-2 (Account Management), CIS 5.3 (Configure access control for remote resources)

Compensating: For organizations without IAM: (1) query web server and application logs for API tokens or session cookies issued to Telus Digital integrations (grep for Telus-related service accounts in /var/log/auth.log or Windows Event ID 4624); (2) manually identify shared credentials in password manager or config files and change them in both your system and Telus Digital's vendor portal; (3) terminate active SSH sessions to Telus Digital systems using `who`, `w`, and `pkill -9 -f ` on Unix; (4) reset API keys in your application configuration and redeploy.

Evidence: Capture BEFORE rotation: (1) Active directory logon events (Windows Event ID 4624, 4625) for past 30 days filtered on Telus Digital service accounts to identify last successful and failed authentications; (2) API audit logs or application logs showing the last use timestamp and originating IP for each Telus Digital integration; (3) session tokens from memory or session store (if accessible) to document what is currently active; (4) SSH host key fingerprints from known_hosts files to establish baseline for detection of credential misuse post-breach.

Step 4, Stakeholder Notification: Notify affected internal teams (legal, compliance, privacy officer) and assess regulatory reporting obligations under applicable frameworks (PIPEDA, GDPR if EU data subjects involved).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis) and §4.1 (Post-Incident Activities — lessons learned)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IR-2 (Incident Response Team), CIS 19.7 (Conduct incident response)

Compensating: Create a two-tier notification: (1) Internal escalation via pre-existing incident response contact list (document this list in your IR plan if not already present); send notification via phone and email simultaneously to ensure immediate awareness; (2) Compliance assessment: use a simple checklist mapping jurisdictions where your data subjects reside (PIPEDA for Canada, GDPR for EU, state laws for US) to applicable notification timelines and thresholds (e.g., GDPR requires notification to DPA if breach affects significant number of residents). If you lack legal counsel, contact your cyber insurance carrier — they often provide legal hotline support.

Evidence: Preserve BEFORE notification: (1) Data subject count and categories: run a query on your customer/employee database filtered by Telus Digital data processor role and export a summary (do not include PII in the summary); (2) timestamp of when Telus Digital first notified your organization and your initial discovery or confirmation of breach scope; (3) any communication from Telus Digital outlining what data classes were accessed/exfiltrated (store in secure location for legal review).

Step 5, Third-Party Risk Review: Audit BPO and data processor relationships for access controls, data minimization practices, and contractual security requirements; update vendor risk assessments for Telus Digital pending breach scope confirmation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4.1 (Post-Incident Activities — review and lessons learned) and NIST 800-53 IA-2 (Authentication)

Controls: NIST 800-53 SA-9 (External Information System Services), NIST 800-53 SA-12 (Supply Chain Risk Management), CIS 6.1, 6.2, 6.3 (Third-party security management)

Compensating: Without a formal vendor risk management platform: (1) Create a spreadsheet inventory of all BPOs/data processors with columns: vendor name, data categories shared, contract renewal date, last security audit date, MFA required (yes/no), data encryption in transit/at rest (yes/no), breach notification timeline in days; (2) for each vendor, request (or review on file) their most recent SOC 2 Type II report or equivalent security attestation; (3) update your procurement/contract management system to flag all processor contracts for security requirements review before next renewal; (4) establish a 6-month re-assessment cycle for high-risk vendors (those holding PII or payment data).

Evidence: Gather BEFORE vendor risk updates: (1) Historical security assessment questionnaires (SAQs) or vendor security scorecards for Telus Digital and peer vendors (if available in your vendor management system); (2) any prior audit or penetration test results showing access control findings or data leakage risks; (3) logs of data transfers to/from Telus Digital (volume, frequency, data classification) to quantify exposure; (4) incident history: check if Telus Digital appears in public breach disclosures or regulatory filings from the past 3 years.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) have been publicly attributed to this incident at time of reporting. Detection focus should be on third-party exposure, not internal compromise, unless your organization has direct system integration with Telus Digital. Recommended detection and monitoring steps: (1) Search email and DLP logs for any data flows to or from Telus Digital-owned domains or known BPO infrastructure. (2) Monitor dark web and underground forum alerts (via your threat intelligence platform or manual monitoring) for datasets matching your employee or customer PII patterns attributed to this breach. (3) If credentials shared with Telus Digital systems exist, monitor for anomalous authentication events using those credentials (T1078 detection: unusual login times, geolocations, or access patterns). (4) Review cloud storage access logs if your organization shares data in cloud repositories accessible to Telus Digital (T1530 relevance). (5) Monitor ShinyHunters-attributed forum activity for sample data releases that could confirm whether your organization's data is included. Source quality for this incident is T3 (trade press and community reporting); treat all scope claims as unverified until Telus Digital publishes official breach notifications.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs attributed to this incident in available public reporting`	ShinyHunters listed alleged stolen data on underground forums; no specific infrastructure IOCs have been publicly confirmed as of current reporting	LOW

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1**
- **6.2**
- **5.2**

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
BleepingComputer	https://www.bleepingcomputer.com/news/security/telus-digital-confir...	T3
Telus Digital confirms breach after hacker claims 1 petabyte data	https://www.reddit.com/r/cybersecurity/comments/1rsp17i/telus_digit...	T3
Telus Digital confirms breach where 'almost 1 petabyte ... - TechRadar	https://www.techradar.com/pro/security/telus-digital-confirms-breac...	T3
Telus Digital data breach confirmed: ShinyHunters claims 1PB theft	https://www.bitdefender.com/en-us/blog/hotforsecurity/telus-digital...	T3
Telus Digital hit with massive data breach | CSO Online	https://www.csoonline.com/article/4144560/telus-digital-hit-with-ma...	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 2026-03-29 18:39 UTC by TJS Security Command Center