INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

Ericsson US Data Breach via Third-Party Service Provider

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0003
Type	Data Breach
Severity	HIGH
Affected Products	Ericsson US subsidiary — employee and customer personal information; approximately 15,000 individuals reported affected
Published	2 days ago

Executive Summary

Ericsson's US subsidiary disclosed a data breach affecting approximately 15,000 employees and customers, caused by a compromise of a third-party service provider. Personal information was confirmed exposed; the full scope of data types has not been publicly enumerated. The incident illustrates direct third-party supply chain risk: a vendor's security failure translates into regulatory notification obligations, reputational exposure, and potential liability for the primary organization.

Technical Analysis

The breach originated at an unnamed third-party service provider with access to Ericsson US systems or data, consistent with MITRE ATT&CK T1199 (Trusted Relationship) as the initial access vector. Attacker activity likely involved credential abuse (T1078, Valid Accounts) and data access from cloud or externally hosted storage (T1530, Data from Cloud Storage). CWE-359 (Exposure of Private Personal Information to an Unauthorized Actor) classifies the resulting data exposure. No CVE has been assigned; this is a breach incident, not a discrete software vulnerability. No CVSS or EPSS scores apply. Specific data types compromised have not been fully disclosed in public reporting as of available sources. No patch is applicable, remediation centers on third-party access controls and data minimization. Sources are Tier 3 (industry press) with a source quality score of 0.56; primary vendor disclosure or regulatory filings should be treated as authoritative when available.

Action Checklist

1. Step 1, Immediate: Audit all third-party vendors with access to employee or customer PII; suspend or restrict access for any provider that cannot confirm breach status or has not completed a recent security review.

2. Step 2, Detection: Review access logs and data egress records for integrations connected to the affected service provider or any provider handling similar data; look for anomalous bulk data access or export events (reference T1530, T1078).

3. Step 3, Assessment: Inventory which vendors hold copies of your organization's employee or customer PII; confirm contractual breach notification obligations are in place and verify whether any shared infrastructure overlaps with the Ericsson US provider chain.

4. Step 4, Communication: If your organization has a vendor relationship with Ericsson or the unnamed third-party provider, notify your privacy, legal, and compliance teams; evaluate whether regulatory notification (GDPR, state breach notification laws) is triggered for your own data.

5. Step 5, Long-term: Strengthen third-party risk management controls, enforce least-privilege access for vendors, require SOC 2 or equivalent attestation, implement continuous monitoring for vendor access activity, and update vendor contracts to include breach notification SLAs aligned to NIST SP 800-161r1 supply chain risk management guidance.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal immediately if any evidence of data exfiltration from your organization's PII repositories is detected during Step 2 analysis, or if vendor inventory reveals shared infrastructure with the Ericsson US third-party provider and your organization holds EU resident data (GDPR notification deadline: 72 hours from discovery).
Recovery Notes	Post-containment: (1) Perform a vendor audit close-out (confirm all high-risk vendors have either been suspended or passed re-certification); (2) implement the vendor risk scorecard and continuous monitoring baseline (query baseline metrics before introducing active monitoring to avoid alert fatigue); (3) conduct a lessons-learned session with legal, privacy, compliance, IT, and security leadership within 30 days; document the incident timeline, root cause, detection gaps, and control gaps (reference NIST 800-61r3 §4.2); (4) update vendor procurement templates to mandate SOC 2 Type II and breach notification SLA language before contract execution.
Forensic Artifacts	Windows Event Log: Event ID 4656 (file/object access), 4663 (file system access), 5140 (network share access), 4688 (process creation for vendor service accounts) | Database audit logs: MSSQL error log, PostgreSQL pg_log, MySQL general_query_log, or Oracle audit trail (query type, source IP, user, row count, timestamp) | API gateway or web application firewall logs: HTTP method, endpoint, authentication source, request/response size, timestamp | Firewall and proxy logs: source IP, destination IP, destination port, protocol, bytes in/out, timestamp for connections to vendor infrastructure | Active Directory audit logs and group membership exports: vendor service account creation date, group membership, last login, privilege changes

Per-Action IR Details

Step 1, Immediate: Audit all third-party vendors with access to employee or customer PII; suspend or restrict access for any provider that cannot confirm breach status or has not completed a recent security review.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation and prevention); §4.1 (supply chain risk context)

Controls: NIST 800-53 SA-9 (external information system services), NIST 800-53 SA-12 (supply chain protection), CIS 6.2 (vendor access controls)

Compensating: Generate a vendor access matrix using spreadsheet: columns for vendor name, data classification (PII/PHI/financial), access mechanism (API/database/file share), last attestation date. Cross-reference against your Identity and Access Management (IAM) tool or Active Directory group membership; for each vendor, query AD groups with 'vendor' or provider name in the group description and list members. Use 'net group "[vendor-group]" /domain' on a domain controller to enumerate access. Compile findings in a single control sheet and timestamp before any suspension. Export screenshots of each query result as evidence.

Evidence: Capture before suspension: (1) Current Active Directory group membership listings for all vendor-affiliated service accounts (export via 'Get-ADGroupMember' PowerShell cmdlet with timestamp); (2) recent access logs from file shares, databases, and APIs serving PII (Windows Event ID 4656, 4663 for file access; application logs for API calls); (3) last attestation or SOC 2 report dates for each vendor (from contracts or email records); (4) screenshot of IAM user/group audit report with creation and last-modified dates; (5) network firewall rules or proxy logs showing outbound connections to vendor infrastructure (source IP, destination IP, port, protocol, byte count).

Step 2, Detection: Review access logs and data egress records for integrations connected to the affected service provider or any provider handling similar data; look for anomalous bulk data access or export events (reference T1530, T1078).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (log analysis and data analysis); §3.2.4 (data exfiltration indicators)

Controls: NIST 800-53 AU-12 (audit and accountability), NIST 800-53 CA-7 (continuous monitoring), CIS 8.2 (audit log monitoring), CIS 8.5 (alert on unusual activity)

Compensating: Manually parse application logs and firewall logs using grep and awk on Unix/Linux or findstr and PowerShell on Windows. Query database access logs (if available) for SELECT queries against tables containing PII (run: 'SELECT * FROM database_audit_log WHERE table_name IN ("users", "customers", "employees") AND event_type = "SELECT" ORDER BY row_count DESC LIMIT 100'). For file share access, export SMB logs from domain controllers (Event ID 5140 = network share access) and filter by vendor service account names and timestamps around the breach discovery date ± 90 days. Use free tools: Splunk Free, Graylog Open Source, or ELK Stack to ingest logs; run queries for data volume anomalies (e.g., 'bytes_transferred > 1GB in 1 hour' per service account). Document baseline data access patterns for each vendor integration over the past 12 months before executing analysis.

Evidence: Preserve before analysis: (1) Complete Windows Event Log 4656 (file/object access attempt), 4663 (file system object access), and 5140 (network share object accessed) for the 90-day window around breach discovery; (2) application-level audit logs from database management systems (e.g., PostgreSQL pg_log, MySQL general_query_log, MSSQL error log) showing source IP, user, query type, row count, and timestamp; (3) firewall/proxy logs with source IP, destination IP, destination port, bytes in/out, and protocol for all connections to vendor infrastructure; (4) API gateway or web application firewall logs showing authentication (user/service account), endpoint, HTTP method, request size, and response size; (5) network traffic captures (PCAP files) from network taps or IDS/IPS systems for data exfiltration time windows, focusing on protocols like HTTPS POST, FTP, SFTP, or SMB to external IPs.

Step 3, Assessment: Inventory which vendors hold copies of your organization's employee or customer PII; confirm contractual breach notification obligations are in place and verify whether any shared infrastructure overlaps with the Ericsson US provider chain.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation) and §4.1 (supply chain risk); NIST SP 800-161r1 §3 (supply chain risk management processes)

Controls: NIST 800-53 SA-3 (system development life cycle), NIST 800-53 PS-7 (third-party personnel security), NIST 800-53 SA-9 (external information system services), CIS 1.1 (vendor and hardware inventory)

Compensating: Create a vendor data inventory spreadsheet: columns for vendor name, data categories held (employee names/SSN, customer PII, financial records), data location (on-prem, cloud SaaS, hybrid), contract

start/end date, breach notification clause (yes/no), and SOC 2/ISO 27001 attestation status. Cross-reference against: (1) procurement records and master service agreements (query email for contract PDFs); (2) data flow diagrams from architecture or security documentation; (3) public vendor announcements and news for disclosed breaches (search vendor name + 'breach' on news aggregators); (4) LinkedIn or company website to identify shared infrastructure (e.g., same cloud region, same managed security provider). Store findings in a single control document with dates and sources. For Ericsson-specific overlap, contact your Ericsson relationship manager and ask directly: 'Does our integration use the same third-party service provider involved in the US subsidiary breach?'

Evidence: Capture before assessment: (1) Current copies of all vendor Master Service Agreements (MSAs) and Data Processing Agreements (DPAs), with breach notification clauses highlighted; (2) IT asset inventory (CMDB) listing all vendors, their access scope, and data classifications they handle; (3) data flow diagrams or architecture documentation showing vendor integration points; (4) procurement records and vendor onboarding checklists showing SOC 2/ISO attestation status and dates; (5) email thread or ticket showing most recent vendor attestation or security review completion date; (6) vendor security questionnaires (VSQs) or completed assessment forms (CAIQ, C3M) with attestation dates.

Step 4, Communication: If your organization has a vendor relationship with Ericsson or the unnamed third-party provider, notify your privacy, legal, and compliance teams; evaluate whether regulatory notification (GDPR, state breach notification laws) is triggered for your own data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.6 (incident notification); NIST SP 800-188 (de-identification guidance); state breach notification laws (varies by jurisdiction)

Controls: NIST 800-53 IR-6 (incident reporting), NIST 800-53 IR-7 (incident handling assistance and support), CIS 6.3 (communication protocols)

Compensating: Document the notification decision process in a shared incident log (e.g., shared Drive folder, wiki, or email thread with legal/privacy/compliance teams copied). Before notifying external parties, determine: (1) Does your organization hold data on EU residents? If yes, GDPR Articles 33-34 require notification to DPA within 72 hours if breach poses 'risk to the rights and freedoms of natural persons.' (2) Does your organization hold data on US residents? Check state laws: California (CCPA, CPRA), New York (SHIELD Act), Massachusetts (105 CMR 17.00), and others require notification 'without unreasonable delay' (typically 30-45 days). (3) Consult your Data Protection Officer (DPO) or privacy counsel before proceeding. Create a notification timeline: decision date, notification recipients, distribution method, and confirmation of receipt. Use email with read receipts or a formal incident notification template signed by authorized leadership.

Evidence: Preserve before communication: (1) Written determination document stating whether breach notification is triggered (reference specific law, threshold met, and risk assessment); (2) list of affected individuals (counts by data category: SSN holders, email addresses, customer records, employee records); (3) internal incident report with discovery date, root cause, containment status, and impact scope; (4) vendor breach announcement or official statement from Ericsson US or the third-party provider (screenshot/archive); (5) email correspondence with legal, privacy, and compliance teams confirming notification decision and timeline; (6) notification template or draft message to regulators and affected individuals (if triggered), with draft date and approval signatures.

Step 5, Long-term: Strengthen third-party risk management controls, enforce least-privilege access for vendors, require SOC 2 or equivalent attestation, implement continuous monitoring for vendor access activity, and update vendor contracts to include breach notification SLAs aligned to NIST SP 800-161r1 supply chain risk management guidance.

NIST Phase: Recovery

Reference: NIST SP 800-161r1 §3 (supply chain risk management); NIST 800-61r3 §4.2.1 (lessons learned); NIST 800-53 SA-9 and SA-12

Controls: NIST 800-53 SA-3 (system development life cycle), NIST 800-53 SA-9 (external information system services), NIST 800-53 SA-12 (supply chain protection), NIST 800-53 CA-7 (continuous monitoring), CIS 1.1 (inventory), 6.2 (vendor access), 8.5 (monitoring)

Compensating: Implement a vendor risk scorecard: create a spreadsheet with vendor name, data access scope, SOC 2 Type II attestation status (yes/no/expired), last security review date, breach history (yes/no), and contractual SLA for breach notification (e.g., '24 hours'). Schedule quarterly reviews; for each vendor, request updated SOC 2 reports (free sources: vendor website, audit firm portal, or direct request). Enforce least-privilege by implementing a 'vendor access request' workflow: every 90 days, re-certify each vendor's access via email to the vendor and the data owner; if no response within 14 days, suspend access. For continuous monitoring without EDR, use free/low-cost tools: (1) Osquery (open-source endpoint agent) to monitor vendor service account activity on critical systems; (2) Splunk Free to index logs from all systems with vendor access and alert on anomalies (baseline data volume per vendor, then alert if exceeded by >50%); (3) manual monthly access reviews: query AD group membership, database user roles, and API key usage for each vendor and compare to previous month. Update vendor MSAs to include: 'Vendor shall notify Ericsson customer of security incident affecting customer data within 24 hours of discovery; failure to notify within 24 hours incurs contract penalties at [X]% of annual contract value.' Store updated contracts in a centralized repository and track renewal dates.

Evidence: Preserve at project start: (1) Current vendor inventory (names, access scope, data classifications); (2) copies of all SOC 2 Type II reports and attestation dates (validate expiration dates); (3) baseline access activity logs for each vendor (30-day average before policy implementation); (4) documented least-privilege access policy (which data, which vendor, which roles); (5) email approvals from data owners and IT leadership confirming policy acceptance; (6) draft updated vendor MSA language for breach notification SLAs and review notes from legal; (7) incident log from this Ericsson breach (root cause, detection date, impact, lessons learned) to reference in lessons-learned session and vendor communication.

Detection Guidance

No confirmed IOCs have been published for this incident. Detection focus should be on third-party access behavior rather than specific indicators. Review SIEM and CASB logs for: bulk data access or export events initiated by service account or API credentials belonging to third-party integrations; access outside normal business hours or from unexpected geolocations tied to vendor accounts (T1078); large data transfers to external storage endpoints (T1530). Query identity logs for service accounts granted access to PII repositories, flag any that accessed records at volume inconsistent with normal operations in the 30-90 days prior to disclosure. If your organization uses shared infrastructure or SSO federation with the affected provider, treat federated sessions as potentially compromised and force re-authentication. No specific log query templates can be provided without knowledge of your SIEM platform and data schema.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1199** — Trusted Relationship

NIST-800-53R5

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

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
SecurityWeek	https://www.securityweek.com/thousands-affected-by-ericsson-data-br...	T3
Ericsson Breach Exposes Data of 15k Employees and Customers	https://www.infosecurity-magazine.com/news/ericsson-breach-exposes-...	T3
Ericsson US discloses data breach after service provider hack	https://www.bleepingcomputer.com/news/security/ericsson-us-disclose...	T3
Ericsson data breach exposes employee and customer information	https://www.scworld.com/brief/ericsson-data-breach-exposes-employee...	T3

Source	URL	Tier
Ericsson US reveals employee and customer data breach after third ...	https://www.techradar.com/pro/security/ericsson-us-reveals-employee...	T3

Generated 2026-03-29 18:43 UTC by TJS Security Command Center