INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-02 06:46 UTC

Trellix Source Code Repository Breach Raises Supply Chain Concerns for Enterprise Security Customers

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0109
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Trellix (formerly McAfee Enterprise / FireEye), source code repository; specific product versions not disclosed
Published	2026-05-02T02:41:00
Discovery Source	Rss

Executive Summary

Trellix has confirmed unauthorized access to a portion of its internal source code repository. The breach affects a major enterprise security vendor whose product lineage spans McAfee Enterprise and FireEye tooling, creating supply chain risk for organizations that depend on Trellix products for endpoint, network, and threat detection. No exploitation of the exposed code has been confirmed, but exposure of proprietary detection logic may enable threat actors to develop evasion techniques targeting Trellix-protected environments.

Technical Analysis

Trellix confirmed unauthorized access to an internal source code repository. No specific product versions or repository scope have been disclosed. The company states its software release and distribution pipeline shows no evidence of compromise, but the forensic investigation remains active. Applicable weaknesses include CWE-284 (Improper Access Control) and CWE-285 (Improper Authorization), consistent with unauthorized repository access, and potentially CWE-312 (Cleartext Storage of Sensitive Information) if credentials or sensitive artifacts were co-located in the repository. No CVE has been assigned. CVSS base score is not applicable; this incident is a supply chain exposure rather than a deployed, exploitable vulnerability. Qualitative severity is assessed as High based on potential downstream impact. MITRE ATT&CK techniques relevant to this incident include T1213 (Data from Information Repositories), T1552.001 (Credentials In Files), T1195.002 (Compromise Software Supply Chain), T1078 (Valid Accounts), and T1059 (Command and Scripting

Interpreter). These techniques reflect the breach vector and potential future attacker exploitation path, not confirmed post-breach attacker activity. No patch is applicable; vendor remediation status and scope of exposed code remain undisclosed. No IOCs have been published. Primary corroborating sources for this breach should be sourced from Trellix's official incident statement; secondary verification is pending.

Action Checklist

1. Step 1: Containment. Inventory all Trellix products deployed in your environment (endpoint agents, network sensors, SIEM connectors, ePolicy Orchestrator instances). Use your network inventory and port scanning to confirm any Trellix management interfaces (ePolicy Orchestrator or equivalent) are not exposed on public-facing networks. Flag any management interfaces accessible without multi-factor authentication for immediate access review. Restrict administrative access to Trellix consoles to known, authorized accounts only.
2. Step 2: Detection. Monitor Trellix product telemetry for anomalous behavior: unexpected rule changes, detection logic modifications, unsigned update packages, or agent communications to non-standard endpoints. Review authentication logs for Trellix management interfaces for unauthorized or unusual access patterns (logins from unexpected IP ranges, interactive service account use, access outside business hours). Cross-reference any Trellix-sourced alerts against a secondary detection control to catch potential evasion.
3. Step 3: Eradication. No patch addresses the source code exposure itself. Vendor remediation is required at the source (securing their repository and investigating scope). Ensure Trellix product update channels are verified as legitimate and that software integrity checks (code signing validation) are enforced before applying any future Trellix updates.
4. Step 4: Recovery. Once Trellix discloses specific product versions and scope, validate the integrity of affected installations by confirming version hashes against vendor-published checksums. Until scope is clarified, maintain current product versions and establish a watch cadence for vendor updates. Monitor Trellix's official advisory channel and incident communications weekly until Trellix declares the investigation closed and issues a final scope disclosure.
5. Step 5: Post-Incident. This incident exposes a control gap in supply chain risk management for security tooling vendors. Review your vendor security assessment process: confirm Trellix (and other critical security vendors) are included in third-party risk reviews. Evaluate whether your detection coverage has compensating controls that do not depend solely on Trellix visibility. Document the incident in your third-party risk register and schedule a formal review if Trellix discloses exploitation evidence.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if Trellix issues an advisory confirming that exposed source code has been used to develop working evasion techniques, if your environment shows Trellix agent binaries with hash mismatches against vendor-published values, or if you operate in a regulated industry (healthcare, finance, critical infrastructure) where compromise of a security monitoring tool may trigger breach notification obligations under HIPAA, PCI-DSS, or NERC CIP.

Recovery Notes	Recovery for this incident is bounded by Trellix's investigation timeline, not a patch cycle — maintain the weekly advisory review cadence and do not stand down elevated monitoring until Trellix issues a formal final scope disclosure confirming no weaponization of exposed code. Sustain the hash-baseline integrity checks on Trellix binaries as a permanent operational control, not a temporary one, given that supply chain risk from this exposure persists for the product lifecycle. If Trellix subsequently releases any product update covering components whose source code was confirmed exposed, treat that update as high-priority and re-validate binary hashes post-installation before restoring normal update automation.
Forensic Artifacts	ePO Audit Log export (Menu > Reporting > Audit Log in ePolicy Orchestrator console): captures all policy changes, DAT content updates, administrator logins, and server task modifications — the primary artifact for detecting unauthorized changes to Trellix detection logic or update configurations post-breach. | Trellix/McAfee Agent logs on endpoints (C:\ProgramData\McAfee\Agent\logs\MA.log on Windows; /var/McAfee/agent/logs/ on Linux): records agent-to-ePO communication events, update receipts, and policy application — critical for identifying agents that received updates from non-standard or spoofed update sources. | Trellix ENS (Endpoint Security) and HX agent binary hash manifest: SHA-256 hashes of all files under C:\Program Files\McAfee\ and C:\ProgramData\McAfee\ compared against Trellix-published release checksums — the primary artifact for detecting tampered or substituted Trellix binaries on endpoints. | Windows Security Event Log (Event ID 4624/4625/4648) filtered on ePO service account names and the ePO server FQDN: documents authentication events against Trellix management infrastructure, surfacing unauthorized access attempts to ePO consoles that could indicate adversary interest in modifying detection policies. | Network flow or pcap data capturing outbound connections from Trellix agent processes (masvc.exe, xagt.exe, mfemactl.exe) to non-Trellix IP ranges: exposes any agent beaconing to adversary-controlled infrastructure that could indicate a compromised update package or modified agent binary introduced via the supply chain.

Per-Action IR Details

Step 1: Containment — Inventory all Trellix products deployed in your environment (endpoint agents, network sensors, SIEM connectors, ePolicy Orchestrator instances). Flag any externally facing Trellix management interfaces for immediate access review. Restrict administrative access to Trellix consoles to known, authorized accounts only.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-8 (System Component Inventory), NIST AC-6 (Least Privilege), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Run 'Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*Trellix*" -or $_.Name -like "*McAfee*" -or $_.Name -like "*FireEye*"}' on all Windows endpoints to enumerate installed Trellix components. On Linux: 'dpkg -l | grep -iE "trellix|mcafee|fireeye"' or 'rpm -qa | grep -iE "trellix|mcafee|fireeye"'. Cross-reference output against a manually maintained asset spreadsheet. For ePolicy Orchestrator (ePO) exposure: run 'netstat -an | findstr :8443' (default ePO HTTPS port) or ':8444' to identify externally listening ePO instances. Use nmap from a jump host: 'nmap -p 8443,8444,8080 ' to confirm which hosts are exposing ePO management interfaces.

Evidence: Before restricting access, capture a full snapshot of current Trellix ePO administrator account list via ePO console export (System Tree > Users) and export to CSV for baseline comparison. Capture Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) filtered on ePO service account names and the ePO server hostname for the 30 days prior to containment action. Preserve ePO server IIS access logs (default path: C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\Logs\) and Apache/Tomcat logs if applicable, covering the same 30-day window, to establish a pre-restriction authentication baseline.

Step 2: Detection — Monitor Trellix product telemetry for anomalous behavior: unexpected rule changes, detection logic modifications, unsigned update packages, or agent communications to non-standard endpoints. Review authentication logs for Trellix management interfaces for unauthorized or unusual access. Cross-reference any Trellix-sourced alerts against a secondary detection control to catch potential evasion.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy a Sigma rule targeting Trellix/McAfee agent process trees: monitor for 'masvc.exe', 'McTray.exe', 'mfemactl.exe', or 'xagt.exe' (FireEye/Trellix HX agent) spawning unexpected child processes or making outbound connections to non-Trellix infrastructure. Use Sysmon Event ID 3 (Network Connection) filtered on those process names and compare destination IPs against Trellix's published update infrastructure ranges. For unsigned update detection: use PowerShell 'Get-AuthenticodeSignature ' against any .DAT or .ZIP files in Trellix update staging directories (default: C:\ProgramData\McAfee\Agent\Data\). Use Wireshark or 'tcpdump -i eth0 host -w trellix_traffic.pcap' to capture and baseline agent-to-ePO communication patterns, flagging any agent beacon traffic to non-ePO IP addresses.

Evidence: Capture Trellix ePO audit log (accessible via ePO console: Menu > Reporting > Audit Log) covering all policy changes, DAT/content updates, and administrator actions for the 60 days prior to the breach disclosure. Export Trellix agent activity logs from endpoints (default path: C:\ProgramData\McAfee\Agent\logs\MA.log) and Trellix ENS (Endpoint Security) logs (C:\ProgramData\McAfee\Endpoint Security\Logs\) for review. Collect network flow data showing outbound connections from Trellix agent processes to document baseline C2 channels and identify deviations. For FireEye/Trellix HX deployments: export host audit logs from the HX console for all enrolled endpoints covering agent update events.

Step 3: Eradication — No patch is available or applicable to this incident. The risk vector is upstream: source code exposure enabling future evasion development, not a deployed vulnerability. Ensure Trellix product update channels are verified as legitimate and that software integrity checks (code signing validation) are enforced before applying any future Trellix updates.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Enforce code signing validation for all Trellix update packages before deployment using PowerShell: 'Get-AuthenticodeSignature "*.DAT" | Where-Object {$_.Status -ne "Valid"}' — any non-valid result should block the update and trigger review. Verify Trellix update server DNS resolution consistently resolves to documented Trellix-owned IP ranges (published in Trellix KB articles); use 'Resolve-DnsName update.nai.com' or equivalent and compare against Trellix's documented infrastructure. Configure ePO to require manual approval for content updates during the elevated-risk period: in ePO, navigate to Automation > Server Tasks and disable automatic DAT pull tasks, replacing with a supervised pull workflow that includes hash verification against Trellix's published DAT checksums (available on the Trellix Security Updates page).

Evidence: Before modifying update configurations, preserve the current ePO Server Task configuration (export task list and schedules from ePO > Automation > Server Tasks) and the current DAT version manifest. Document the current Trellix update channel URLs configured in ePO (Menu > Configuration > Registered Servers) to establish a pre-change baseline. Capture the Windows Registry key 'HKLM\SOFTWARE\McAfee\Agent\' and 'HKLM\SOFTWARE\WOW6432Node\McAfee\' on representative endpoints to document current agent configuration and update source settings before any changes are applied.

Step 4: Recovery — Validate the integrity of your current Trellix product installations by confirming version hashes against vendor-published checksums. Monitor Trellix's official advisory channel and incident

communications for updates on investigation scope. Establish a watch cadence — at minimum weekly — until Trellix declares the investigation closed and issues a final scope disclosure.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Generate SHA-256 hashes of all installed Trellix binaries on representative endpoints using: 'Get-FileHash "C:\Program Files\McAfee*" -Algorithm SHA256 -Recurse | Export-Csv trellix_hash_baseline.csv'. Compare against Trellix's published file hashes in their product release notes or security advisories. For Linux-based Trellix components (e.g., ENS for Linux, MVISION EDR sensor): use 'sha256sum /opt/McAfee/agent/bin/*' and compare against vendor documentation. Set a calendar-driven review cadence using a shared team task in your ticketing system (Jira, ServiceNow, or even a shared calendar) tied to Trellix's official advisory page (https://www.trellix.com/en-us/about/newsroom/stories/research/ — verify this URL manually as it is not from a pre-verified reference list) and Trellix's customer support portal for investigation updates.

Evidence: Preserve the hash baseline CSV generated during integrity validation as a dated forensic artifact — this serves as the verified-good state for future comparison if Trellix later discloses that specific binaries were compromised. Retain ePO event logs and agent communication logs collected during the detection phase as long-term artifacts; do not purge these logs until Trellix issues a final scope disclosure, consistent with NIST AU-11 (Audit Record Retention). Document the date and content of each Trellix advisory update reviewed during the watch cadence in your incident tracking record.

Step 5: Post-Incident — This incident exposes a control gap in supply chain risk management for security tooling vendors. Review your vendor security assessment process: confirm Trellix (and other critical security vendors) are included in third-party risk reviews. Evaluate whether your detection coverage has compensating controls that do not depend solely on Trellix visibility. Document the incident in your third-party risk register and schedule a formal review if Trellix discloses exploitation evidence.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-12 (Supply Chain Protection), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Map your current detection coverage to MITRE ATT&CK and identify which detections are exclusively Trellix-sourced: use MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/ — verify URL manually) to layer your Trellix-covered techniques and visually identify gaps. For each gap, deploy a free compensating control: Sysmon with the SwiftOnSecurity or Olaf Hartong config for process/network telemetry, Sigma rules converted to native Windows Event Log queries via 'sigma convert', or osquery with CIS-provided query packs for endpoint state visibility. Add Trellix to your vendor risk register with a 'SOURCE CODE BREACH — ELEVATED' flag and set a formal reassessment trigger upon any Trellix advisory update disclosing evasion tool development or exploitation of the exposed code.

Evidence: Compile a post-incident artifact package for the third-party risk register entry: include the initial breach disclosure date, your environment's Trellix product inventory (from Step 1), the hash baseline (from Step 4), the ePO audit log export (from Step 2), and a record of all Trellix advisories reviewed during the watch cadence. This package constitutes the evidentiary record for any future regulatory inquiry or customer disclosure requirement if Trellix later confirms that exposed source code was weaponized against your environment. Retain this package per your organization's incident record retention policy, minimum consistent with NIST AU-11 (Audit Record Retention).

Detection Guidance

No published IOCs are available at this time. Focus detection on behavioral indicators rather than signatures. Key monitoring areas: (1) Trellix management console authentication logs - look for logins from unexpected IP ranges, service accounts used interactively, or access outside business hours; (2) Trellix agent update events - flag any updates that arrive outside scheduled maintenance windows or fail code signature validation; (3) Detection rule changes - alert on any modification to Trellix detection policies not initiated through your change management process; (4) Network traffic from Trellix agents - baseline normal C2 communication patterns and alert on connections to new or unrecognized endpoints; (5) Secondary control comparison - if Trellix is your primary endpoint or network detection layer, validate its alerting against an independent control (EDR, SIEM correlation from a different data source) to identify potential blind spots introduced by evasion techniques developed from the exposed source code. No SIEM query templates are possible without confirmed IOCs or exploitation indicators.

Framework Mappings

MITRE-ATTACK

- **T1587.001** — Malware
- **T1552.001** — Credentials In Files
- **T1195.002** — Compromise Software Supply Chain
- **T1213** — Data from Information Repositories
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts

NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

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

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1587.001	Malware	Resource-Development
T1552.001	Credentials In Files	Credential-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1213	Data from Information Repositories	Collection
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/trellix-confirms-source-code-brea...	T3
Vulnerability Scan Results - Trellix Software Release 9.0.0	https://thrive.trellix.com/s/article/000003259?language=en_US	T3

Source	URL	Tier
Trellix - Vulnerability Disclosure Program | HackerOne	https://hackerone.com/trellix/policy_versions	T3
Trellix / McAfee is worst : r/cybersecurity - Reddit	https://www.reddit.com/r/cybersecurity/comments/1hwh966/trellix_mca...	T3
Vulnerability Reasonable Disclosure Policy - Trellix	https://www.trellix.com/advanced-research-center/advanced-threat-re...	T3