INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-30 06:56 UTC

Mozilla Root Store Policy v3.1 Tightens CA Transparency and Compliance Requirements

GOVERNANCE | MEDIUM | CVSS 5.0

SCC Item ID	SCC-GOV-2026-0088
Type	Governance
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Mozilla Firefox Root Store, all Certificate Authorities trusted by Mozilla; effective July 1, 2026
Published	2026-06-29T11:33:46+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Mozilla published Root Store Policy v3.1, effective July 1, 2026, raising governance and transparency standards for all Certificate Authorities (CAs) trusted by Firefox. Organizations operating web-facing infrastructure rely on publicly trusted certificates; if a CA fails to meet the updated requirements and Mozilla removes it from the trusted root store, certificates issued by that CA will be rejected by Firefox and by the many Linux distributions and open-source tools that consume the Mozilla CA bundle. Enterprise PKI and vendor management teams should confirm their CAs are on track for compliance before the effective date.

Technical Analysis

Mozilla Root Store Policy v3.1 (effective July 1, 2026) raises requirements for CAs included in the Firefox trusted root store across three areas: certificate transparency (CT) logging obligations, audit rigor, and incident reporting timelines. The policy is a governance update, not a discrete vulnerability disclosure; no CVE has been assigned. The associated CWE references, CWE-295 (Improper Certificate Validation), CWE-297 (Improper Validation of Certificate with Host Mismatch), and CWE-326 (Inadequate Encryption Strength), identify the weakness classes this policy is designed to reduce structurally across the public Web PKI. MITRE techniques in scope include T1553.004 (Install Root Certificate), T1557 (Adversary-in-the-Middle), T1539 (Steal Web Session Cookie), and T1588.004 (Digital Certificates). CAs that fail compliance face distrust actions; downstream impact extends beyond Firefox to any system consuming the Mozilla CA bundle, including many Linux distributions and open-source tooling stacks. No exploited vulnerability is present; risk is compliance-driven and timeline-bound.

Action Checklist

1. Step 1: Inventory, identify every publicly trusted certificate in your environment and confirm which CA issued each one. Cross-reference issuing CAs against the Mozilla CA Certificates in Firefox report (available at the Common CA Database / CCADB portal: ccadb.my.salesforce-sites.com/mozilla/CACertificatesInFirefoxReport) to flag any CA currently under compliance review or subject to a Mozilla incident report.
2. Step 2: CA Compliance Assessment, contact each issuing CA's compliance or account team before July 1, 2026 to confirm they have attested compliance with Root Store Policy v3.1, specifically covering CT logging obligations, updated audit requirements, and incident reporting timelines. Request written confirmation or point to their public CCADB disclosure.
3. Step 3: Certificate Transparency Verification, confirm all certificates issued after the effective date carry valid Signed Certificate Timestamps (SCTs) from CT logs accepted under the new policy. Use tools such as crt.sh or your CA's CT log dashboard to validate SCT coverage for critical web-facing services.
4. Step 4: Contingency Planning, for any CA that cannot confirm v3.1 compliance, develop a re-issuance plan through an alternate compliant CA before July 1, 2026. Prioritize internet-facing services, API endpoints, and any system where certificate distrust would cause service disruption or supply-chain breakage. Reference NIST AC-17 (Remote Access) and AC-20 (Use of External Systems) when documenting third-party CA dependency risk.
5. Step 5: Post-Effective-Date Monitoring, after July 1, 2026, monitor Mozilla Security Blog and the mozilla.dev.security.policy Google Group for distrust announcements. Set alerts on certificate expiry and CA status changes. Document this policy update in your vendor risk register under the relevant CA relationships and schedule a review at the next quarterly GRC cycle. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for ongoing monitoring cadence.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if Mozilla publicly announces a distrust action or opens a formal CCADB incident report against any CA that has issued certificates currently deployed in your environment, or if a CA cannot provide written v3.1 compliance attestation within 30 days of contact, as either condition creates a hard July 1, 2026 re-issuance deadline with potential Firefox-enforced service rejection affecting internet-facing revenue or regulated-data flows.
Recovery Notes	After re-issuing certificates through a confirmed v3.1-compliant CA, validate SCT presence and CT log inclusion for every replaced certificate using crt.sh and openssl before returning services to production. Monitor web server and load balancer TLS handshake error rates for at least 72 hours post-swap to detect any client rejection caused by intermediate CA chain misconfigurations or missing SCTs. Schedule a follow-up CCADB spot-check 90 days after July 1, 2026 to confirm that all CAs in your inventory have maintained their compliance status, as Mozilla may take additional enforcement actions against CAs that initially attested compliance but subsequently fail audits.

Forensic Artifacts	Point-in-time PEM certificate chain captures (`openssl s_client -connect :443 -showcerts`) for all internet-facing services, timestamped at inventory baseline, pre-migration, and post-migration — establishes chain of custody for certificate lineage if a CA distrust dispute arises | CCADB report CSV snapshots with download timestamps for each CA in your inventory, preserving the compliance status of each CA at specific dates before and after July 1, 2026 | Written CA compliance attestation emails or CCADB disclosure URLs with retrieval dates, constituting the vendor risk evidentiary record if a CA is later distrusted despite having claimed v3.1 compliance | Web server and load balancer TLS handshake error logs (e.g., Apache SSL_ERROR_RX_RECORD_TOO_LONG, Nginx SSL_do_handshake errors, or HTTP 526 responses from CDN/proxy layers) post-July 1, 2026, which would indicate Firefox-enforced rejection of certificates from a distrusted CA | crt.sh JSON query outputs for each monitored domain showing SCT count, log operator names, and SCT timestamps, retained as the detection record demonstrating CT compliance status at the time of verification

Per-Action IR Details

Step 1: Inventory — identify every publicly trusted certificate in your environment and confirm which CA issued each one. Cross-reference issuing CAs against the Mozilla CA Certificates in Firefox report (ccadb.my.salesforce-sites.com/mozilla/CACertificatesInFirefoxReport) to flag any CA currently under compliance review or subject to a Mozilla incident report.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and asset visibility before an adverse event (CA distrust action) occurs

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), NIST AC-20 (Use of External Systems)

Compensating: Run `openssl s_client -connect :443 /dev/null | openssl x509 -noout -issuer -subject -dates` against each internet-facing endpoint and pipe results to a CSV. Automate across host lists with a short bash loop. Cross-reference issuer O= and CN= values against the CCADB report downloaded as a CSV from ccadb.my.salesforce-sites.com. A two-person team can cover hundreds of endpoints in an afternoon using this approach with GNU parallel.

Evidence: This step does not alter live state; no volatile capture is required before execution. However, retain point-in-time snapshots of certificate chain outputs (full PEM chains via `openssl s_client -showcerts`) and the CCADB report CSV with its download timestamp, as these establish the pre-remediation baseline if a CA is later distrusted and incident timelines are audited.

Step 2: CA Compliance Assessment — contact each issuing CA's compliance or account team before July 1, 2026 to confirm they have attested compliance with Root Store Policy v3.1, specifically covering CT logging obligations, updated audit requirements, and incident reporting timelines. Request written confirmation or point to their public CCADB disclosure.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Identifying and remediating weaknesses in third-party dependencies before they become incidents; aligns with pre-incident vendor risk assessment

Controls: NIST AC-20 (Use of External Systems), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Download each CA's current CCADB entry directly from ccadb.my.salesforce-sites.com and review the 'Standard Audit' and 'BR Audit' fields for audit period currency and the 'Policy Documentation' field for v3.1 attestation language. Document findings in a shared spreadsheet with columns: CA name, CCADB audit date, v3.1 attestation confirmed (Y/N), written confirmation received (Y/N), follow-up deadline. No SIEM required — this is a manual governance workflow achievable by one analyst.

Evidence: No live system state is altered by this step; volatile capture is not applicable. Preserve all written CA responses, CCADB record screenshots with timestamps, and any CA-published CP/CPS documents referencing Root Store Policy v3.1 compliance. These records constitute the evidentiary basis for vendor risk decisions and any future dispute if a CA is distrusted after having claimed compliance.

Step 3: Certificate Transparency Verification — confirm all certificates issued after the effective date carry valid Signed Certificate Timestamps (SCTs) from CT logs accepted under the new policy. Use tools such as crt.sh or your CA's CT log dashboard to validate SCT coverage for critical web-facing services.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyzing the environment to determine whether certificates in use satisfy updated policy requirements, identifying non-compliant certificates before Firefox enforces distrust

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Query crt.sh for each domain using `curl -s 'https://crt.sh/?q=&output=json' | jq '.[] | {id, issuer_name, not_before, not_after}'` and verify SCT fields are present. For local certificate inspection, run `openssl x509 -in cert.pem -noout -text | grep -A5 'CT Precertificate SCTs'` to confirm embedded SCTs. Flag any certificate lacking at least two SCTs from distinct CT log operators, as Mozilla Root Store Policy v3.1 tightens multi-log SCT requirements.

Evidence: This step is read-only and does not alter live state; no volatile capture precedes it. Preserve the full JSON output from crt.sh queries and the openssl text output for each certificate examined, timestamped, as the detection record. If a certificate is found to lack valid SCTs post-July 1, 2026, this output is the artifact demonstrating non-compliance at a specific point in time for GRC and audit purposes.

Step 4: Contingency Planning — for any CA that cannot confirm v3.1 compliance, develop a re-issuance plan through an alternate compliant CA before July 1, 2026. Prioritize internet-facing services, API endpoints, and any system where certificate distrust would cause service disruption or supply-chain breakage. Reference NIST AC-17 (Remote Access) and AC-20 (Use of External Systems) when documenting third-party CA dependency risk.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Executing preventive containment before a CA distrust event causes service rejection; isolating dependency on a non-compliant CA by migrating to a confirmed-compliant issuer

Controls: NIST AC-17 (Remote Access), NIST AC-20 (Use of External Systems), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Maintain a prioritized re-issuance queue in a shared spreadsheet ranked by service criticality (public HTTPS endpoints first, internal mTLS second, code-signing last). Use Let's Encrypt (via Certbot) as a free, ACME-compatible, Mozilla-trusted CA for internet-facing services that do not require OV/EV certificates: `certbot certonly --standalone -d `. For OV/EV requirements, obtain quotes and compliance attestations from at least two alternate CAs before committing. Document each service's re-issuance status and target completion date at least 30 days before July 1, 2026 to allow for propagation and testing.

Evidence: Before replacing any certificate on a live service, capture the current TLS handshake in full using `openssl s_client -connect :443 -showcerts` and save the complete certificate chain as a PEM file with a timestamp in the filename. This preserves the pre-migration certificate chain for audit trail continuity and for comparison if a CA later claims the original certificate was compliant. No volatile memory state is implicated by certificate replacement, but web server access logs immediately surrounding the certificate swap should be archived to document continuity of service.

Step 5: Post-Effective-Date Monitoring — after July 1, 2026, monitor Mozilla Security Blog and the mozilla.dev.security.policy Google Group for distrust announcements. Set alerts on certificate expiry and CA status changes. Document this policy update in your vendor risk register under the relevant CA relationships and schedule a review at the next quarterly GRC cycle. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for ongoing monitoring cadence.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Implementing continuous monitoring and lessons-learned processes aligned to CSF [GV, ID] functions; updating vendor risk posture based on CA compliance outcomes after the policy effective date

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Subscribe to the mozilla.dev.security.policy Google Group via email digest (free, no tooling required) and create a filtered inbox rule to flag messages containing 'distrust', 'removal', or the name of any CA in your inventory. For certificate expiry alerting without a SIEM, use a cron-scheduled bash script calling `openssl s_client -connect :443 /dev/null | openssl x509 -noout -enddate` against your endpoint list and email the team when any certificate expires within 30 days. Update your vendor risk register entry for each CA relationship with the July 1, 2026 compliance attestation date and set a calendar reminder for the Q3 2026 GRC review.

Evidence: No live state is altered by ongoing monitoring; volatile capture is not applicable. Maintain a dated log of all Mozilla Security Blog posts and mozilla.dev.security.policy threads reviewed, CA CCADB status checks with retrieval timestamps, and any distrust announcements affecting CAs in your inventory. If a CA distrust event occurs post-July 1, 2026, Firefox rejection errors in web server and load balancer access logs (HTTP 526 or TLS handshake failures) and browser console SSL errors reported by users constitute the primary operational evidence of impact.

Detection Guidance

No IOCs exist for this governance update; detection focus is on compliance posture and potential downstream certificate distrust events. Monitor the following: (1) Certificate Transparency logs via crt.sh or your CA's dashboard for SCT issuance gaps on your domains after July 1, 2026. (2) Browser console errors and TLS handshake failures in application and web server logs that indicate a certificate is no longer trusted (HTTP 526, SSL_ERROR_BAD_CERT_DOMAIN, or equivalent). (3) Mozilla Security Blog and mozilla.dev.security.policy mailing list for distrust announcements against your issuing CAs. (4) CCADB public records for audit findings or incident reports filed by your CAs. Per NIST AU-6, these sources should be reviewed on a defined frequency; weekly review is appropriate for organizations with significant public-facing certificate inventory. No SIEM-based IOC queries apply to this governance item; the relevant signal is CA compliance status and certificate chain validation results.

Framework Mappings

MITRE-ATTACK

- **T1557** — Adversary-in-the-Middle
- **T1553.004** — Install Root Certificate
- **T1539** — Steal Web Session Cookie
- **T1588.004** — Digital Certificates

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

NIST-800-53R5

- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates

- **SC-13** — Cryptographic Protection

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access
T1553.004	Install Root Certificate	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1588.004	Digital Certificates	Resource-Development

Sources

Source	URL	Tier
Mozilla Security Blog	https://blog.mozilla.org/security/2026/06/29/improving-transparency...	T1
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-gr...	T1
CA Certificates In Firefox	https://ccadb.my.salesforce-sites.com/mozilla/CACertificatesInFiref...	T3
Trusted PEM distribution of Mozilla's CA bundle - Google Groups	https://groups.google.com/g/mozilla.dev.security.policy/c/FYIBEF_AVMI	T3

Generated 2026-06-30 06:56 UTC by TJS Security Command Center