INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-16 18:59 UTC

Microsoft's Original Secure Boot Certificate Nears End of Life: What Enterprises Must Do Before the Clock Runs Out

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0062
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows (all editions relying on original UEFI Secure Boot certificate infrastructure; broad Windows enterprise ecosystem)
Published	2026-04-16T11:16:30
Discovery Source	Rss

Executive Summary

Microsoft's original Secure Boot certificate, a foundational component of Windows boot integrity, is nearing expiration, requiring enterprises to transition to new certificate trust before the deadline or risk leaving endpoints unable to verify bootloader integrity. This is not a vulnerability in the traditional sense, but the security consequence of inaction is equivalent: unprotected systems become susceptible to bootkit and firmware-level attacks that operate below the operating system, evading most conventional endpoint defenses. The transition signals a broader reality for enterprise security teams: certificate lifecycle management is now a first-order operational risk, not a background IT task.

Technical Analysis

Secure Boot is a UEFI firmware feature that validates each component of the boot chain, from the bootloader through the kernel, against a set of trusted certificates before execution. Microsoft's original Windows Production CA 2011 certificate serves as the root trust anchor in this chain for a substantial portion of the Windows ecosystem. As this certificate approaches end of life, any system that has not been updated to trust its replacement will lose the ability to validate bootloader signatures against the original certificate, effectively disabling Secure Boot's integrity guarantees for that trust chain.

The attack surface this opens maps directly to MITRE ATT&CK techniques for pre-OS persistence: T1542 (Pre-OS Boot) covers the general bootkit threat class, with T1542.001 (System Firmware) and T1542.003 (Bootloader) covering the specific persistence locations adversaries target when Secure Boot is absent or

misconfigured. T1553.006 (Subvert Trust Controls: Code Signing Policy Modification) reflects how adversaries exploit weakened certificate validation, and T1195.003 (Supply Chain Compromise: Compromise Hardware Supply Chain) captures the firmware supply chain angle, a concern for organizations running hardware with outdated or unpatched UEFI implementations.

The underlying weakness classes are CWE-295 (Improper Certificate Validation), CWE-324 (Use of a Key Past its Expiration Date), and CWE-347 (Improper Verification of Cryptographic Signatures). None of these require an active adversary to cause harm; configuration drift and patch lag are sufficient. Note: This is not a CVE or traditional vulnerability; Secure Boot functionality depends on certificate lifecycle management rather than patch remediation. Risk assessment should be based on exposure conditions and regulatory requirements, not CVSS scoring.

Microsoft documented the transition in a support article covering Secure Boot certificate update status in the Windows Security app, which received an update indicator in the April 2026 cumulative release. CrowdStrike's Falcon for IT published tooling to support certificate lifecycle management at scale, allowing enterprise teams to query and remediate certificate trust status across large endpoint fleets. The source material indicates this is a coordinated lifecycle action, not an emergency patch cycle, but the operational window for remediation is finite and the consequences of missing it are material.

Action Checklist

1. Step 1: Assess exposure, audit all Windows endpoints, servers, and virtual machines to determine which rely on the original Microsoft Windows Production CA 2011 Secure Boot certificate; prioritize systems running older Windows editions or hardware with infrequently updated UEFI firmware
2. Step 2: Review controls, verify that cumulative updates through April 2026 (or later) have been applied to all in-scope systems; confirm UEFI firmware updates are current for hardware vendors in your fleet, as certificate trust is managed at both the OS and firmware layer
3. Step 3: Validate certificate status, use the Secure Boot certificate update status indicator in the Windows Security app (see https://support.microsoft.com/en-us/topic/secure-boot-certificate-update-status-in-the-windows-security-app-5ce39986-7dd2-4852-8c21-ef30dd04f046) or CrowdStrike Falcon for IT's certificate lifecycle tooling to confirm new certificate trust is established on each endpoint before relying on self-reporting alone
4. Step 4: Update threat model, add Secure Boot certificate expiration as a standing item in your certificate lifecycle risk register; map the exposure to T1542 (Pre-OS Boot) and T1553.006 in your threat register to contextualize it for red team and detection engineering teams
5. Step 5: Communicate findings, brief leadership on the operational deadline and the specific consequence of inaction: endpoints that miss the transition lose boot integrity validation, which undermines a key defense-in-depth control against persistent, pre-OS threats such as bootkits
6. Step 6: Monitor developments, track Microsoft's official support documentation and Windows Update history for any extensions, phased enforcement timelines, or additional guidance; assign ownership of the certificate lifecycle workstream to a named team before the expiration window closes

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal/compliance if post-audit results from Step 1 reveal that systems processing PII, PHI, or financial data will not complete the Secure Boot certificate transition before the expiration deadline, as unprotected endpoints in those environments introduce a pre-OS persistence vector that may trigger breach notification obligations under HIPAA, PCI-DSS, or applicable state privacy laws if subsequently compromised by a bootkit.
Recovery Notes	After confirming new Microsoft UEFI CA 2023 certificate enrollment on all in-scope endpoints via Step 3 validation queries, conduct a 30-day monitoring period targeting Windows Security Center Secure Boot status via Event ID 1796 in Microsoft-Windows-Kernel-Boot/Operational to detect any post-update regressions caused by firmware rollbacks, failed cumulative updates, or system replacements that re-introduce legacy certificate state. Any endpoint returning to Microsoft Windows Production CA 2011 as sole trust anchor after the transition deadline should be treated as a potential indicator of tampering and triaged under the T1542 (Pre-OS Boot) playbook before being returned to production. Maintain the pre-transition Secure Boot db snapshots collected in Step 1 for a minimum of 12 months as forensic baseline evidence.
Forensic Artifacts	Windows Event Log — Microsoft-Windows-Kernel-Boot/Operational, Event ID 1796: logs Secure Boot database state and policy at each boot cycle; a system anchored solely to Microsoft Windows Production CA 2011 post-transition deadline will produce distinguishable policy entries from systems that have successfully enrolled Microsoft UEFI CA 2023 | UEFI NVRAM Secure Boot variables (db, dbx, KEK, PK) extracted via PowerShell Get-SecureBootUEFI: the raw certificate enrollment state per machine; pre- and post-transition snapshots provide forensic proof of whether the new trust anchor was successfully written to firmware or whether the system retained legacy-only enrollment | Windows Update log (Get-WindowsUpdateLog output, %USERPROFILE%\Desktop\WindowsUpdate.log): documents whether the specific cumulative update KB delivering the Secure Boot certificate trust update was successfully installed, failed, or was rolled back — critical for distinguishing missed-patch from active-tampering scenarios | Win32_BIOS WMI class output (SMBIOSBIOSVersion, ReleaseDate fields): firmware version string per endpoint providing evidence of whether hardware-layer UEFI updates that embed the new Secure Boot certificate were applied; a firmware version predating the vendor's UEFI CA 2023 update release indicates the system remains at risk at the firmware layer regardless of OS patch state | Windows Security Center API state for Secure Boot (accessible via PowerShell or WMI through SecurityCenter2 namespace): provides the self-reported Secure Boot status visible to the OS; discrepancy between this self-reported state and the raw UEFI variable state collected above would be a high-fidelity indicator of bootkit-level manipulation of the Secure Boot enforcement path, consistent with T1542 (Pre-OS Boot) TTPs

Per-Action IR Details

Step 1: Assess exposure — audit all Windows endpoints, servers, and virtual machines to determine which rely on the original Microsoft Windows Production CA 2011 Secure Boot certificate; prioritize systems running older Windows editions or hardware with infrequently updated UEFI firmware

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: asset inventory and exposure baselining prior to an anticipated integrity-impacting event

Controls: NIST IR-4 (Incident Handling) — establishes requirement for preparation activities including asset-scope identification before an incident occurs, NIST SI-2 (Flaw Remediation) — identifies obligation to inventory systems with known remediation requirements, applicable here to certificate trust gaps, NIST CM-8 (System Component Inventory)

— requires maintaining an accurate inventory of system components, including firmware and boot configuration state, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — mandates tracking of all enterprise assets with attributes sufficient to identify UEFI firmware version and OS edition, CIS 2.2 (Ensure Authorized Software is Currently Supported) — covers identification of endpoints running OS versions or firmware no longer receiving Secure Boot certificate trust updates

Compensating: Run the following PowerShell one-liner across all Windows endpoints via WinRM or SCCM script: `Confirm-SecureBootUEFI` returns True/False for Secure Boot state; supplement with `(Get-SecureBootPolicy).Publisher` to surface the active policy anchor. For firmware version enumeration without SCCM, use: `Get-WmiObject -Class Win32_BIOS | Select-Object Manufacturer, SMBIOSBIOSVersion, ReleaseDate` piped to a CSV. For VMs, query Hyper-V hosts with `Get-VMFirmware -VMName * | Select-Object VMName, SecureBootTemplate` to identify VMs using the 'MicrosoftWindows' template (which anchors to the legacy CA). Aggregate results in a spreadsheet segmented by OS build number and hardware vendor.

Evidence: Before conducting the audit, snapshot the current Secure Boot Database (db, dbx, KEK, PK) state on a representative sample of endpoints using the PowerShell command `Get-SecureBootUEFI db | Format-List` and save output to a timestamped file — this establishes a pre-transition baseline of which certificates are currently enrolled in each machine's UEFI variable store. Also collect UEFI firmware version strings (`Win32_BIOS.SMBIOSBIOSVersion`) per device to document which hardware vendors have and have not shipped updated firmware embedding the new Microsoft UEFI CA 2023 certificate.

Step 2: Review controls — verify that cumulative updates through April 2026 (or later) have been applied to all in-scope systems; confirm UEFI firmware updates are current for hardware vendors in your fleet, as certificate trust is managed at both the OS and firmware layer

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring defensive controls are in place and current before the expiration deadline forces an incident-equivalent state

Controls: NIST SI-2 (Flaw Remediation) — requires testing and applying software updates related to flaw remediation; applies here to Windows cumulative updates that deploy the new Secure Boot certificate trust chain, NIST SI-7 (Software, Firmware, and Information Integrity) — mandates integrity verification tools and firmware integrity checks, directly applicable to UEFI firmware update validation, NIST CM-3 (Configuration Change Control) — governs controlled update and configuration change processes for both OS-layer and firmware-layer Secure Boot certificate changes, CIS 7.3 (Perform Automated Operating System Patch Management) — requires monthly or more frequent OS patching; the April 2026 cumulative update is the critical delivery vehicle for the new Microsoft UEFI CA 2023 trust anchor, CIS 7.4 (Perform Automated Application Patch Management) — extends patch management obligation to firmware; UEFI vendor updates (Dell, HP, Lenovo, etc.) deliver updated Secure Boot databases at the hardware layer

Compensating: For OS patch verification without SCCM/Intune, run: `Get-HotFix | Where-Object {$_.InstalledOn -gt (Get-Date).AddDays(-60)} | Sort-Object InstalledOn | Export-Csv patches.csv` — compare KB numbers against Microsoft's published Secure Boot update history for each OS build. For firmware, use vendor CLI tools at no cost: Dell Command Update (`dcu-cli.exe /scan`), HP Image Assistant (`HPIA.exe /Operation:Analyze`), or Lenovo System Update — all have silent/scriptable modes. For air-gapped or mixed-vendor fleets, manually cross-reference `Win32_BIOS.SMBIOSBIOSVersion` output against each vendor's current BIOS catalog page for that model.

Evidence: Capture Windows Update logs before applying any additional patches: `Get-WindowsUpdateLog` (Windows 10/11) outputs ETW traces to `%USERPROFILE%\Desktop\WindowsUpdate.log` — search for KB entries associated with Microsoft's Secure Boot certificate deployment (reference Microsoft Support KB articles tied to the April 2025–April 2026 cumulative update series). Also preserve the current UEFI db variable state (`Get-SecureBootUEFI db`) before applying firmware updates, as a pre/post comparison will confirm whether the new Microsoft UEFI CA 2023 certificate was successfully enrolled in the UEFI Signature Database after the firmware update.

Step 3: Validate certificate status — use the Secure Boot certificate update status indicator in the Windows Security app (documented at support.microsoft.com) or CrowdStrike Falcon for IT's certificate lifecycle tooling to confirm new certificate trust is established on each endpoint before relying on self-reporting alone

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: verifying control effectiveness and confirming actual trust chain state rather than assumed compliance

Controls: NIST SI-4 (System Monitoring) — requires monitoring systems to detect configuration states inconsistent with security policy, including Secure Boot certificate trust gaps, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — requires analysis of system configuration state data to identify anomalous or non-compliant conditions, NIST CA-7 (Continuous Monitoring) — mandates ongoing monitoring of security control effectiveness; certificate trust state is a security control that must be verified, not assumed, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — requires verification that remediation actions have been completed and controls are effective, CIS 8.2 (Collect Audit Logs) — audit log collection underpins the ability to verify Secure Boot state changes and detect systems that failed to complete the certificate transition

Compensating: Without CrowdStrike Falcon for IT, use PowerShell for scaled validation: `Confirm-SecureBootUEFI` confirms Secure Boot is enabled; `Get-SecureBootUEFI db | Select-String -Pattern 'Microsoft UEFI CA 2023'` (after exporting db to readable form via `Format-Hex` or third-party UEFI tools like `UEFITool` CLI) confirms the new certificate is enrolled. For fleet-scale enumeration without a commercial tool, deploy as a scheduled task via Group Policy or run via PSRemoting: `Invoke-Command -ComputerName (Get-Content servers.txt) -ScriptBlock {Confirm-SecureBootUEFI}`. For firmware-layer verification, use `msinfo32.exe` output (BIOS Version/Date field) collected via SCCM hardware inventory or a simple WMI query script to validate firmware versions match post-update baselines.

Evidence: Query the Windows Event Log on each endpoint for Event ID 1796 in the Microsoft-Windows-Kernel-Boot/Operational channel, which logs Secure Boot policy and database state at boot time — entries here will reveal whether the active Secure Boot db includes the new Microsoft UEFI CA 2023 certificate or is still anchored solely to the expiring Microsoft Windows Production CA 2011. Additionally, collect output of `Get-SecureBootUEFI KEK` and `Get-SecureBootUEFI PK` to document the full trust hierarchy, not just the signature database, since a partial or incomplete certificate enrollment can leave the chain broken even if Secure Boot reports as enabled.

Step 4: Update threat model — add Secure Boot certificate expiration as a standing item in your certificate lifecycle risk register; map the exposure to T1542 (Pre-OS Boot) and T1553.006 in your threat register to contextualize it for red team and detection engineering teams

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: integrating threat intelligence into risk registers and detection engineering pipelines to maintain proactive defensive posture

Controls: NIST IR-4 (Incident Handling) — requires that incident handling capability encompass preparation activities including threat modeling and control gap analysis, NIST RA-3 (Risk Assessment) — mandates identification and assessment of risks including those arising from configuration or certificate lifecycle gaps that reduce boot integrity assurance, NIST SI-5 (Security Alerts, Advisories, and Directives) — requires disseminating and acting on security advisories; mapping Microsoft's Secure Boot advisory to ATT&CK techniques operationalizes the advisory for detection teams, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — certificate lifecycle risk belongs in the vulnerability management process as a standing tracked item, not a one-time remediation, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation strategy must account for the pre-OS threat surface exposed by Secure Boot certificate expiration

Compensating: Without a commercial threat intelligence platform, document the ATT&CK mapping directly in a shared spreadsheet or wiki: T1542 (Pre-OS Boot) covers bootkit persistence that Secure Boot is designed to block; T1553.006 (Code Signing — Subvert Trust Controls) covers adversary abuse of weakened or expired certificate trust chains. Feed this mapping to detection engineering by creating a Sigma rule stub targeting Event ID 1796 anomalies and Windows Security Center API state changes for Secure Boot. For red team context, reference public bootkit PoC research (e.g., BlackLotus, CosmicStrand) that specifically exploits weakened Secure Boot enforcement — these represent the realistic threat class that certificate expiration enables.

Evidence: Before finalizing the threat model entry, collect a snapshot of the current Secure Boot enforcement policy via `Get-SecureBootPolicy` on representative endpoints — the Policy.Publisher and Policy.PolicyVersion fields indicate whether systems are operating under Microsoft's standard or custom Secure Boot policy, which affects which ATT&CK sub-techniques are most directly applicable. Also document which endpoints in your fleet have previously triggered

Secure Boot violation events (Event ID 1796 with non-zero violation codes in Microsoft-Windows-Kernel-Boot/Operational) as these represent historically at-risk systems warranting prioritized treatment in the threat model.

Step 5: Communicate findings — brief leadership on the operational deadline and the specific consequence of inaction: endpoints that miss the transition lose boot integrity validation, which undermines a key defense-in-depth control against persistent, pre-OS threats such as bootkits

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing communication structures and ensuring leadership understands operational risk before a deadline-driven incident state is reached

Controls: NIST IR-6 (Incident Reporting) — requires timely reporting of security-relevant conditions to appropriate organizational personnel, including leadership, before escalation thresholds are crossed, NIST IR-8 (Incident Response Plan) — IR plan must include communication procedures; briefing leadership on a pending deadline with known security consequences is a plan-required activity, NIST PM-9 (Risk Management Strategy) — senior leadership must be informed of risks that materially affect the organization's security posture; Secure Boot expiration meets this threshold given its pre-OS attack surface implications, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation requires leadership buy-in for resource allocation; communication of the consequence of inaction (bootkit susceptibility) is required to obtain that buy-in

Compensating: Without a GRC platform for formal risk communication, prepare a one-page executive brief using a free template structured around: (1) deadline date, (2) affected asset count from Step 1 audit, (3) specific attack scenario enabled by inaction — reference publicly documented bootkits such as BlackLotus (which exploited CVE-2022-21894 to bypass Secure Boot) as the threat class that Secure Boot certificate integrity blocks, (4) remediation cost/effort estimate from Steps 2–3, (5) residual risk if deadline is missed. Attach the ATT&CK mapping from Step 4 as an appendix for technical leadership. Use Microsoft's official advisory language to anchor severity claims rather than internal estimates.

Evidence: Before the leadership brief, assemble quantified exposure data from previous steps: total endpoint count relying on Microsoft Windows Production CA 2011 (from Step 1), count of systems not yet updated through the April 2026 cumulative update threshold (from Step 2), and count of systems where new certificate trust has not been confirmed (from Step 3). These numbers constitute the evidentiary basis for the risk communication and should be treated as forensic artifacts — version-controlled and timestamped — since they may be referenced in post-incident reviews if any systems are later compromised via pre-OS attack vectors.

Step 6: Monitor developments — track Microsoft's official support documentation and Windows Update history for any extensions, phased enforcement timelines, or additional guidance; assign ownership of the certificate lifecycle workstream to a named team before the expiration window closes

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: institutionalizing lessons learned, updating processes, and assigning ownership to prevent recurrence of certificate lifecycle gaps

Controls: NIST IR-4 (Incident Handling) — post-incident improvements must include updated handling procedures for certificate lifecycle events, with named ownership, NIST IR-8 (Incident Response Plan) — IR plan must be reviewed and updated following significant security events or near-miss conditions; the Secure Boot transition represents a near-miss that warrants plan updates covering certificate expiration scenarios, NIST SI-5 (Security Alerts, Advisories, and Directives) — requires ongoing monitoring of external security advisories from Microsoft and UEFI forum sources; this is the standing mechanism for tracking Microsoft's Secure Boot enforcement timeline updates, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — certificate lifecycle monitoring must be embedded in the documented vulnerability management process with assigned ownership, not treated as a one-time project, CIS 7.2 (Establish and Maintain a Remediation Process) — standing remediation process must include certificate lifecycle as a recurring risk category with defined review cadence

Compensating: Without a commercial threat intelligence feed, configure free monitoring using: (1) RSS feed subscription to Microsoft Security Update Guide (`https://msrc.microsoft.com/update-guide/releaseNote/rss`) filtered for Secure Boot and UEFI terms; (2) CISA Known Exploited Vulnerabilities catalog RSS

(`https://www.cisa.gov/known-exploited-vulnerabilities-catalog`) for any future KEV entries related to Secure Boot bypass; (3) a simple cron job or scheduled task running weekly that queries `winver` and patch level against a maintained baseline CSV and emails delta reports to the named owner. Document the workstream owner, review cadence, and escalation path in the IR plan as a named certificate lifecycle runbook.

Evidence: At workstream handoff, transfer all forensic artifacts collected during Steps 1–5 to the named owning team: the pre-transition Secure Boot db variable snapshots, firmware version baselines, patch compliance CSVs, Event ID 1796 log extracts, and the ATT&CK-mapped risk register entry. These artifacts serve as the post-transition baseline — any future deviation from confirmed new-certificate-enrolled state on a given endpoint (detectable via the same PowerShell queries) represents a regression requiring immediate investigation under the T1542/T1553.006 threat model documented in Step 4.

Detection Guidance

Query your endpoint management platform (SCCM, Intune, or equivalent) for systems that have not received cumulative updates through April 2026; these are the most likely candidates for unresolved certificate trust gaps. In CrowdStrike Falcon for IT environments, use the published certificate lifecycle query to surface endpoints where the new Secure Boot certificate has not been enrolled.

For hunting, review UEFI and Secure Boot event logs (Windows Event Log channel Microsoft-Windows-Kernel-Boot) for Secure Boot validation failures or policy override events. Consult Microsoft's Windows Event Log documentation for specific Event IDs corresponding to Secure Boot validation failures in your Windows version, as they vary across OS releases. These events flag boot integrity anomalies that warrant immediate investigation. A cluster of Secure Boot validation failures across endpoints in the same hardware cohort may indicate either a missed patch cycle or, in a worst case, active exploitation of weakened boot validation.

Audit TPM attestation logs where available: if your organization uses Windows Hello for Business, Intune device health attestation, or similar TPM-backed posture checks, a change in Secure Boot status will surface as a posture failure before it becomes an incident. Configure alerts on attestation state changes in your MDM or endpoint management console.

For firmware-level risk, query hardware vendor advisories for UEFI firmware updates that reference Secure Boot database (db/dbx) changes; outdated UEFI firmware may not properly honor the new certificate even after OS-level updates are applied. Cross-reference your hardware asset inventory against vendor firmware release notes for the relevant period.

Framework Mappings

MITRE-ATTACK

- **T1195.003** — Compromise Hardware Supply Chain
- **T1542** — Pre-OS Boot
- **T1553.006** — Code Signing Policy Modification
- **T1542.001** — System Firmware
- **T1542.003** — Bootkit

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
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195.003	Compromise Hardware Supply Chain	Initial-Access
T1542	Pre-OS Boot	Defense-Evasion
T1553.006	Code Signing Policy Modification	Defense-Evasion
T1542.001	System Firmware	Persistence
T1542.003	Bootkit	Persistence

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/endpoint-security/microsoftoriginal-win...	T3
Microsoft Issues 2026 Secure Boot Warning - LinkedIn	https://www.linkedin.com/pulse/microsoft-introduces-new-secure-boot...	T3
Falcon for IT Supports Windows Secure Boot Certificate Lifecycle ...	https://www.crowdstrike.com/en-us/blog/falcon-for-it-supports-windo...	T3

Source	URL	Tier
April 2026 Update Adds Secure Boot Certificate Status in Windows ...	https://windowsforum.com/threads/april-2026-update-adds-secure-boot...	T3
Secure Boot certificate update status in the Windows Security app	https://support.microsoft.com/en-us/topic/secure-boot-certificate-u...	T1