INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-02 07:15 UTC

Critical Use-After-Free in PQC Hybrid Key-Share Handling, CVE-2026-7531

CVE VULNERABILITY | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0382
Type	CVE Vulnerability
CVE ID	CVE-2026-7531
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0035 (27th percentile)
Affected Products	Microsoft azl3 mariadb 10.11.18-1 on Azure Linux 3.0
Published	2026-07-01T14:48:24
Discovery Source	Msrc Patch Tuesday

Executive Summary

Microsoft disclosed a critical use-after-free vulnerability (CVE-2026-7531, CVSS 9.8) in the post-quantum cryptography hybrid key-share handling code within the azl3 MariaDB 10.11.18-1 package on Azure Linux 3.0, as part of Patch Tuesday June 2026. Organizations running this specific MariaDB package on Azure Linux 3.0 face potential exposure to remote code execution, privilege escalation, or cryptographic material compromise. No confirmed exploitation or active threat actor activity has been reported in the available source data at this time.

Technical Analysis

CVE-2026-7531 is a use-after-free condition (CWE-416) in the post-quantum cryptography (PQC) hybrid key-share handling code within Microsoft's azl3 mariadb 10.11.18-1 package, specific to the Azure Linux 3.0 platform. The vulnerability carries a CVSS base score of 9.8 (Critical). Use-after-free flaws occur when a program continues to reference memory after it has been freed; in a cryptographic key-share context, this can corrupt heap memory in ways that may permit an attacker to achieve remote code execution (MITRE T1203) or privilege escalation (MITRE T1068), or to expose cryptographic keying material. The EPSS score is 0.00346 (approximately 26th percentile), indicating low current exploitation probability relative to the CVSS severity. CISA KEV inclusion has not been confirmed. No public exploit code or active threat actor attribution appears in the available source data. Affected scope is narrowly defined: Microsoft azl3 mariadb 10.11.18-1 on Azure Linux 3.0. Source references include MSRC Update Guide, the MSRC CVRF June 2026 consolidated feed, and the

NVD detail page.

Action Checklist

1. Step 1: Containment, Identify all Azure Linux 3.0 hosts running the azl3 mariadb 10.11.18-1 package. If internet-facing MariaDB instances cannot be immediately patched, restrict inbound access to known trusted IP ranges at the network layer and disable unnecessary remote connections in the MariaDB configuration. Consult the MSRC Update Guide for CVE-2026-7531 for vendor-specific interim mitigations. (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers)
2. Step 2: Detection, Query your asset inventory for Azure Linux 3.0 hosts with the azl3 mariadb package at version 10.11.18-1 (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.1, Establish and Maintain a Software Inventory). Review system and MariaDB error logs for anomalous crash signals, unexpected process terminations, or segmentation faults in MariaDB processes, which may indicate memory corruption attempts. Monitor for anomalous privilege escalation events on database hosts (NIST AU-6, Audit Record Review, Analysis, and Reporting; MITRE T1068, T1203). No confirmed IOC patterns are available in the source data at this time.
3. Step 3: Eradication, Apply the vendor-supplied update for CVE-2026-7531 as published by Microsoft via the MSRC Update Guide and the June 2026 Patch Tuesday release. Verify the updated package version resolves the affected azl3 mariadb 10.11.18-1 component on Azure Linux 3.0. Use automated patch management where available (CIS 7.3, Perform Automated Operating System Patch Management; CIS 7.4, Perform Automated Application Patch Management). Rotate any cryptographic keying material that may have been accessible to the vulnerable MariaDB process, given the nature of the PQC key-share exposure vector (D3-CRO, Credential Rotation).
4. Step 4: Recovery, After applying the vendor patch, confirm the updated package version is installed on all affected hosts. Re-enable any network restrictions that were tightened during containment only after patch verification. Review MariaDB and system logs for any indicators of anomalous activity during the exposure window (NIST AU-6, Audit Record Review, Analysis, and Reporting; NIST AU-12, Audit Record Generation). Validate that cryptographic key rotation completed successfully and that PQC hybrid key-share operations are functioning as expected.
5. Step 5: Post-Incident, Document exposure window from patch availability to remediation completion. Assess whether the software inventory process captured this package before disclosure, and close gaps using CIS 2.1 and CIS 2.2 (Ensure Authorized Software is Currently Supported). Evaluate whether PQC-enabled components in third-party packages are included in the vulnerability management scope (CIS 7.1, Establish and Maintain a Vulnerability Management Process). Review privilege and access controls on database hosts to limit blast radius of future memory-corruption vulnerabilities (NIST AC-6, Least Privilege; CIS 5.4, Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP, User Account Permissions).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if any MariaDB crash dump, audit log entry, or memory artifact collected during detection analysis confirms exploitation of CVE-2026-7531 prior to patch application, or if PQC hybrid key-share material stored in the MariaDB data directory is confirmed or suspected to have been exposed — either condition may trigger cryptographic incident notification obligations depending on the classification of data protected by those keys.
Recovery Notes	After patch verification, restore network access controls to pre-incident baselines and monitor MariaDB error logs and Linux audit logs for at least 14 days for any recurrence of segmentation faults, unexpected process restarts, or anomalous privilege escalation events on previously affected Azure Linux 3.0 hosts. Validate that all rotated PQC hybrid key-share material and TLS certificates are functioning correctly in MariaDB TLS negotiation by reviewing connection logs for SSL handshake errors. If any host cannot be confirmed clean from memory analysis (Step 3 evidence), treat it as potentially compromised and reimage before returning to production.
Forensic Artifacts	MariaDB error log (/var/log/mariadb/mariadb.log): contains segmentation fault, SIGSEGV, 'Aborted', or 'stack smashing detected' entries that would be produced by a use-after-free memory corruption event in the PQC hybrid key-share handling code path. | Linux kernel audit log (/var/log/audit/audit.log): syscall records for mmap, mprotect, execve, and clone from the MariaDB process PID during the exposure window — a use-after-free exploit escalating to RCE would produce anomalous mprotect(PROT_EXEC) or execve calls originating from the mariadbd process. | MariaDB process memory dump (gcore or LiME RAM capture): preserves in-memory state of PQC hybrid key-share buffers at the time of potential exploitation, including any freed-but-reused memory regions indicative of the use-after-free condition described in CVE-2026-7531. | Pre-patch mariadbd binary hash and /proc//maps snapshot: establishes whether the vulnerable 10.11.18-1 binary was the active executable and identifies any anomalous executable memory regions (e.g., rwx mappings outside standard library paths) that would indicate shellcode staging following successful use-after-free exploitation. | MariaDB data directory SSL/TLS certificate and key files (/var/lib/mysql/*.pem, paths defined in ssl_cert/ssl_key in /etc/my.cnf.d/server.cnf): the PQC hybrid key-share exposure vector makes these the primary cryptographic assets at risk — their metadata (mtime, atime) and content hashes before and after rotation confirm whether key material was accessed or modified during the exposure window.

Per-Action IR Details

Step 1: Containment — Identify all Azure Linux 3.0 hosts running the azl3 mariadb 10.11.18-1 package. If internet-facing MariaDB instances cannot be immediately patched, restrict inbound access to known trusted IP ranges at the network layer and disable unnecessary remote connections in the MariaDB configuration. Consult the MSRC Update Guide for CVE-2026-7531 for vendor-specific interim mitigations. (NIST AC-4 — Information Flow Enforcement; CIS 4.4 — Implement and Manage a Firewall on Servers)

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On each Azure Linux 3.0 host, run `rpm -qa | grep mariadb` to enumerate affected instances without SIEM. Apply host-level iptables rules to restrict MariaDB port 3306 to trusted CIDR ranges: `iptables -A INPUT -p tcp --dport 3306 ! -s -j DROP`. In MariaDB config (/etc/my.cnf.d/*.cnf), set `bind-address=127.0.0.1` and comment out `skip-networking=0` to disable remote listener on instances that do not require external access.

Evidence: Before restricting network access or modifying MariaDB configuration, capture volatile state: run `ss -tnp | grep 3306` and `netstat -ano | grep 3306` to record all active connections to the MariaDB listener; capture `/proc//net/tcp` for kernel-level socket state; run `lsof -p ` to record open file descriptors and memory-mapped regions

that a use-after-free exploit targeting PQC key-share buffers would have touched; snapshot `ps auxf` to capture the full MariaDB process tree. Save outputs with timestamps before altering any firewall rules or config files.

Step 2: Detection — Query your asset inventory for Azure Linux 3.0 hosts with the azl3 mariadb package at version 10.11.18-1 (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.1 — Establish and Maintain a Software Inventory). Review system and MariaDB error logs for anomalous crash signals, unexpected process terminations, or segmentation faults in MariaDB processes, which may indicate memory corruption attempts. Monitor for anomalous privilege escalation events on database hosts (NIST AU-6 — Audit Record Review, Analysis, and Reporting; MITRE T1068, T1203). No confirmed IOC patterns are available in the source data at this time.

NIST Phase: Detection Analysis

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: Use osquery to enumerate affected hosts fleet-wide: `SELECT name, version FROM rpm_packages WHERE name LIKE '%mariadb%' AND version = '10.11.18-1';`. For crash detection without SIEM, grep MariaDB error logs directly: `grep -iE 'segfault|SIGSEGV|stack smashing|Use-after-free|Aborted|core dumped' /var/log/mariadb/mariadb.log /var/log/messages`. Deploy a Sigma rule targeting Linux audit log entries for unexpected suid/privilege changes (`auditctl -w /usr/bin/mariadbd -p x`) to catch post-exploitation privilege escalation attempts on the database host.

Evidence: This step is read-only analysis and does not alter live state; however, preserve the following before any subsequent containment or eradication actions: collect `/var/log/mariadb/mariadb.log` and `/var/log/mariadb/mariadb-error.log` in full; collect `/var/log/messages` and `journalctl -u mariadb --since ` output; capture Linux audit logs (`/var/log/audit/audit.log`) filtering on syscalls execve, mmap, mprotect, and clone from the MariaDB process PID, which would reflect memory manipulation consistent with use-after-free exploitation; record `/proc//maps` to identify any anomalous executable memory regions loaded by the MariaDB process that could indicate shellcode staging.

Step 3: Eradication — Apply the vendor-supplied update for CVE-2026-7531 as published by Microsoft via the MSRC Update Guide and the June 2026 Patch Tuesday release. Verify the updated package version resolves the affected azl3 mariadb 10.11.18-1 component on Azure Linux 3.0. Use automated patch management where available (CIS 7.3 — Perform Automated Operating System Patch Management; CIS 7.4 — Perform Automated Application Patch Management). Rotate any cryptographic keying material that may have been accessible to the vulnerable MariaDB process, given the nature of the PQC key-share exposure vector (D3-CRO — Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: On Azure Linux 3.0 hosts without automated patch management, apply the fix manually: `tdnf update mariadb` followed by `rpm -q mariadb` to confirm the patched version is installed. After patching, rotate the MariaDB SSL/TLS certificates and any PQC hybrid key-share material stored under MariaDB's data directory (typically `/var/lib/mysql/`): regenerate server certificates using `mariadb-admin` or replace files in the `ssl_cert` / `ssl_key` paths defined in `/etc/my.cnf.d/server.cnf`. For teams without a secrets manager, document the rotation with a timestamped change log entry referencing CVE-2026-7531.

Evidence: Volatile and forensic evidence MUST be captured before patching (which overwrites the vulnerable binary and alters live state): acquire a full memory dump of the running MariaDB process using `gcore ` or LiME kernel module to capture RAM — this preserves in-memory PQC key-share buffer state that a use-after-free exploit would corrupt or expose; record `rpm -qi mariadb` output and hash the current `mysqld`/`mariadbd` binary (`sha256sum /usr/sbin/mariadbd`) before replacement to establish a pre-patch baseline; preserve copies of current SSL/TLS

certificate files and key material from the MariaDB data directory under chain-of-custody before rotation, as these represent the cryptographic assets at risk from the PQC key-share exposure vector.

Step 4: Recovery — After applying the vendor patch, confirm the updated package version is installed on all affected hosts. Re-enable any network restrictions that were tightened during containment only after patch verification. Review MariaDB and system logs for any indicators of anomalous activity during the exposure window (NIST AU-6 — Audit Record Review, Analysis, and Reporting; NIST SI-4 — no mapped control in the provided knowledge base for SI-4 specifically; use AU-6 and AU-12 — Audit Record Generation). Validate that cryptographic key rotation completed successfully and that PQC hybrid key-share operations are functioning as expected.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation)

Compensating: Verify patch deployment across all Azure Linux 3.0 hosts with: `for host in $(cat affected_hosts.txt); do ssh $host 'rpm -q mariadb'; done`. Validate PQC hybrid key-share functionality by reviewing MariaDB startup logs for TLS/SSL negotiation errors post-rotation: `journalctl -u mariadb --since 'patch_timestamp' | grep -iE 'ssl|tls|key|pqc|error'`. Confirm no crash or segfault signals reappear in `/var/log/mariadb/mariadb.log` within 24 hours of service restart post-patch, which would suggest the fix is incomplete or a secondary issue persists.

Evidence: This step does not alter volatile state but requires reviewing evidence already collected: cross-reference the pre-patch MariaDB error log timestamps against the CVE-2026-7531 disclosure date (June 2026 Patch Tuesday) to bound the exposure window; verify that audit log continuity exists for the full exposure window in `/var/log/audit/audit.log` — gaps may indicate log tampering or log rotation misconfiguration that obscures exploitation activity; confirm that newly generated PQC key-share material and SSL certificates are present in the MariaDB data directory and that file hashes differ from pre-rotation baselines, validating rotation actually completed rather than silently failing.

Step 5: Post-Incident — Document exposure window from patch availability to remediation completion. Assess whether the software inventory process captured this package before disclosure, and close gaps using CIS 2.1 and CIS 2.2 (Ensure Authorized Software is Currently Supported). Evaluate whether PQC-enabled components in third-party packages are included in the vulnerability management scope (CIS 7.1 — Establish and Maintain a Vulnerability Management Process). Review privilege and access controls on database hosts to limit blast radius of future memory-corruption vulnerabilities (NIST AC-6 — Least Privilege; CIS 5.4 — Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP — User Account Permissions).

NIST Phase: Post Incident

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

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Produce the exposure window report by diffing the MSRC advisory publication date against the patch-confirmed timestamps collected in Step 4. Update the software inventory (CIS 2.1) to explicitly tag `azl3 mariadb` as a PQC-enabled component so future CVEs affecting PQC hybrid key-share code paths are automatically flagged in vulnerability scans. For privilege review without PAM tooling, run `awk -F: '$3 == 0 {print $1}' /etc/passwd` and `getent group mysql` on each database host to identify accounts with UID 0 or membership in the mariadb service group that violate least-privilege expectations.

Evidence: No volatile evidence capture is required at this phase; preserve the complete incident record: retain the pre-patch `mariadbd` binary hash, the collected memory dump from Step 3, all MariaDB and Linux audit logs spanning the exposure window, and the certificate rotation change log — together these constitute the evidentiary record for a post-incident review board and satisfy AU-11 (Audit Record Retention) requirements. If the organization is subject to breach notification obligations and any PQC key material or data was confirmed or suspected to have been accessed

during the exposure window, flag this package for legal and compliance review before records are archived.

Detection Guidance

Query package management on Azure Linux 3.0 hosts to identify installations of azl3 mariadb at version 10.11.18-1 (e.g., rpm -qa | grep mariadb on RPM-based Azure Linux hosts). Review MariaDB error logs and system journal (journalctl) for segmentation faults, unexpected daemon restarts, or memory corruption signals in mariadbd or related processes, which may indicate attempted exploitation of the use-after-free condition. Monitor for anomalous privilege escalation events on hosts running the affected package, consistent with MITRE T1068 activity. Audit logs should capture unexpected process privilege changes and unusual outbound connections from database hosts (NIST AU-2, Event Logging; NIST AU-12, Audit Record Generation; CIS 8.2, Collect Audit Logs). No confirmed IOCs (hashes, IPs, domains) are present in the available source data. EPSS score of 0.00346 indicates current exploitation probability is low, but the CVSS 9.8 severity warrants proactive detection posture.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1203** — Exploitation for Client Execution

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-7531	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Jun	T1
CVE-2026-7531 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-7531	T1
CVE-2026-7531 Security Vulnerability Analysis & Exploit Details	https://cve.akaoma.com/cve-2026-7531	T3
CVE-2026-7531 - Endor Labs	https://www.endorlabs.com/vulnerability/cve-2026-7531	T3

Generated 2026-07-02 07:15 UTC by TJS Security Command Center