QT9 Security Advisory – [QT9-SA-2025-001]

Date Published: [10/16/2025]
Last Updated: [10/16/2025]
Severity: Medium (per internal assessment)
Status: 16.0 (25.0.24.0)

---

1 Summary

During an authorized white-box assessment conducted for one of our enterprise clients, two vulnerabilities were identified in legacy versions of **QT9-QMS** – On prem software. These vulnerabilities affected older on-premises deployments that had not yet been updated to current security standards. Both issues have been fully remediated in supported releases. No exploitation in customer environments has been observed.

---

2 Affected Products and Versions

Product	Affected Versions	Fixed In	Support Status
QT9-QMS	V12.0 – 16.0 (25.0.24.0)	V16.0 (25.0.24.0)	V16 are End-of-Support (EoS)

---

3 Vulnerability Details

1. Static MACHINEKEY value in IIS configuration

- **Description:**
  Earlier QT9-QMS installers used a default MACHINEKEY entry in web.config.
  Because this key was common across deployments, it could theoretically be used to decrypt or sign ASP.NET ViewState data.
- **Impact:**
  Under certain conditions, this could allow a malicious actor to tamper with serialized data in ViewState, potentially leading to remote code execution (RCE).
- **Resolution:**
  Beginning with **QT9-QMS v16.x** unique cryptographic keys are generated dynamically, eliminating shared key reuse.

---

2. Local File Inclusion (LFI) via filedownload.aspx endpoints

QT9 Security Advisory – [QT9-SA-2025-001]

- **Description:**
  Several legacy endpoints (/customers/filedownload.aspx, /employees/filedownload.aspx, /suppliers/filedownload.aspx, /docportal/filedownload.aspx) could allow unauthenticated file retrieval from the application webroot.
- **Impact:**
  An attacker could potentially access files stored under the application directory, including configuration data.
- **Resolution:**
  The file-handling routines have been redesigned to validate and sanitize file-path inputs and restrict access to authorized, mapped directories. Additional logging and access-control checks have been added.

---

4 Scope Clarification

These findings originated from testing authorized by **a client**, one of QT9's customers.
Testing of other environments or instances of QT9-QMS outside client's deployment was **not authorized by QT9** and is considered out of scope for that engagement.
Vendor boundaries and contractual testing scopes must be observed for any future research.

---

5 Mitigation & Recommendations

- Upgrade to **QT9-QMS v16.x** or later.
- Replace any default or shared IIS MACHINEKEY entries with unique values per instance.
- Disable or restrict direct access to legacy filedownload.aspx endpoints if still present.
- Review webserver hardening guides in QT9's **Security Configuration Baseline** documentation.

---

6 Vendor Disclosure Statement

QT9 follows **ISO/IEC 29147** and **30111** coordinated vulnerability-disclosure practices.
We are working with the **MITRE CVE Program** as part of our CNA onboarding to ensure any public record accurately reflects the impact, affected versions, and remediations already in place.

QT9 Security Advisory – [QT9-SA-2025-001]

7️⃣ Acknowledgments

QT9 thanks **Ian ODette** for identifying and responsibly disclosing the in-scope issues that led to these improvements.

8️⃣ References

- MITRE CVE Program: https://cve.mitre.org

✅ Disclaimer

QT9 issues this advisory to inform customers and partners of remediated vulnerabilities in legacy, end-of-support versions of QT9-QMS. Findings derived from testing outside authorized contractual scope are not recognized as part of this advisory.