RC4 Protocol Update – C•CURE 9000 / iSTAR Pro Impact Assessment

KB Number: 000038628
Published: 17/04/2026

Products Affected

- C•CURE 9000
- iSTAR Pro controllers
- Microsoft Windows Server (host OS context only)

Summary

RC4 is a legacy stream cipher encryption algorithm introduced in 1987 and was historically used to encrypt network communications between C•CURE 9000 and iSTAR Pro controllers. RC4 was implemented as an optional setting through System Variables. Due to multiple security vulnerabilities identified between 2001 and 2015, the use of RC4 in TLS was prohibited in 2015, and formal support for RC4 was removed from C•CURE 9000 in 2022.

Recent Microsoft communications regarding RC4-related changes in Windows Server raised concerns about potential impact to C•CURE 9000 and iSTAR Pro controller communications. Engineering and QA reviews have confirmed that C•CURE 9000 is not impacted by RC4 deprecation. Although RC4-named API calls may still be present, the RC4 encryption algorithm itself is not used by the product.

No code changes are required, and QA validation completed successfully with no issues identified.

Background

Customers and field teams requested clarification on whether the removal or deprecation of RC4 from Windows Server could affect:

- iSTAR controller communication
- C•CURE 9000 functionality
- Existing deployments following Windows updates
  These concerns were driven by unclear external messaging received by customers regarding potential RC4 protocol dependencies.

Technical Clarification

RC4 Encryption vs. RC4-Named API Calls

- C•CURE 9000 does **not** use the RC4 encryption algorithm.

- The system uses certain API calls that include “RC4” in their naming; however, these are not implementations of the RC4 encryption cipher.
- Engineering explicitly reviewed whether Microsoft’s latest updates would continue supporting these API calls.

Engineering & QA Assessment

- Engineering confirmed that RC4-related changes do not impact C•CURE 9000 or iSTAR Pro controllers.
- QA testing was completed with the following results:
- No defects identified
- No regressions observed
- No code changes required

Customer Impact

- No functional impact to existing C•CURE 9000 installations
- No impact to iSTAR controller communications
- No impact to systems updated with recent Microsoft Windows Server patches

Customers can safely proceed with applicable Microsoft updates without concern for RC4-related disruption, based on current validation.

Timeline of Key Communications (Internal)

- Initial inquiry raised regarding RC4 dependency and potential iSTAR impact
- Engineering review initiated to validate API usage versus encryption usage
- Confirmation provided that RC4 encryption is not used
- QA testing completed with no issues identified
- Final confirmation shared that no code changes are required

Recommended Guidance (Public)

- No action is required for C•CURE 9000 customers related to RC4 deprecation.
- This topic should be treated as informational only unless future Microsoft updates explicitly change API support behavior.
- If customers reference external or unclear RC4-related messaging, clarify that:
- C•CURE 9000 does not rely on RC4 encryption.
- The product has been validated through QA testing against current Windows Server updates.