Security Advisories

Welcome to the **linqi** Security Advisory page. The security of our software products and the protection of your data are our highest priorities. On this page, we provide transparent information about identified and resolved security vulnerabilities (CVEs), share technical details, and provide the corresponding patches. We strongly recommend that you install the security updates listed here in your systems in a timely manner.

Would you like to report a vulnerability to us? Please review our Vulnerability Disclosure Policy.

Security Bulletins

Security Advisory: Insecure Direct Object Reference (IDOR) in Comment API in linqi

Advisory ID: SEC-2026-004
Publication Date: June 05, 2026
Status: Resolved

Overview

- **CVE-ID:** CVE-2026-11369
- **Vulnerability Type:** Insecure Direct Object Reference / Missing Authorization (CWE-639, CWE-862)
- **Severity:** High
- **CVSS Base Score:** 7.1

Affected Products

- **linqi – All versions prior to 1.4.8.6**

Vulnerability Description

An Insecure Direct Object Reference (IDOR) vulnerability was identified in the Comment API (`GET /api/Comment` and `POST /api/Comment`) of the affected linqi application versions. The application fails to perform adequate authorization checks to verify that the requesting user has access to the object identified by the `relatedObjectId` parameter.

As a result, any authenticated user can read and write comments on any process across all business units system-wide by supplying an arbitrary object GUID. The root cause is located in the service and controller layers, which pass the caller-supplied `relatedObjectId` directly to the database without first verifying ownership or access rights.

Solution (Patch)

The issue has been completely resolved in version **1.4.8.6**. The update introduces strict ownership validation checks within the controller and service layers prior to any database interactions. We strongly recommend that all customers update their systems to the latest version as soon as possible.

Security Advisory: Improper Authentication Bypass in CDN File Access in linqi

Advisory ID: SEC-2026-003
Publication Date: June 05, 2026
Status: Resolved

Overview

- **CVE-ID:** CVE-2026-11345
- **Vulnerability Type:** Improper Authentication (CWE-287)
- **Severity:** Medium *(Note: Actual security impact is negligible)*
- **CVSS Base Score:** 6.9

Affected Products

- **linqi** OnPremise – **All versions prior to 1.4.8.6**

Vulnerability Description

An Improper Authentication vulnerability was identified in the `/api/Cdn/GetFile` endpoint of the affected linqi versions. A flaw in the internal validation logic allows an unauthenticated, remote attacker to bypass intended file access controls simply by providing an `AnonFile` query parameter containing exactly 256 characters.

Impact Context: While this vulnerability technically allows a bypass of the application's authorization check, **the actual security risk is negligible**. The exposed resources are limited strictly to minified JavaScript and CSS files that contain no sensitive data, secrets, or user information. Furthermore, these static front-end assets are inherently designed to be publicly accessible via a standard Content Delivery Network (CDN).

Solution (Patch)

The issue has been fully resolved in version **1.4.8.6**. The update refactors the authentication logic to remove the length-based bypass and properly validates access against the backend authorization service. While the risk is minimal, we recommend all customers update their systems to the latest version during their next regular maintenance window.

Acknowledgements

We would like to thank **Ianis Bernard from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Server-Side Request Forgery (SSRF) allowing Internal Network Probing

Advisory ID: SEC-2026-002
Publication Date: June 05, 2026
Status: Resolved

Overview

- **CVE-ID:** CVE-2026-11346
- **Vulnerability Type:** Server-Side Request Forgery (SSRF) (CWE-918)
- **Severity:** Medium
- **CVSS Base Score:** 5.3

Affected Products

- **linqi** OnPremise – **All versions prior to 1.4.8.6**

Vulnerability Description

A Server-Side Request Forgery (SSRF) vulnerability has been identified in the custom process creation feature of the affected application versions. By crafting a specific process that includes an HTTP Request component, an authenticated user can force the application server to send arbitrary HTTP requests to internal network components.

While direct data extraction is not possible, an attacker can infer the status of internal system ports (e.g., open, closed, or filtered) by observing variations in the application's response behavior (such as returning a Success message, a Failed message, or a 504 Gateway Time-out). This flaw enables unauthorized internal network reconnaissance.

Solution (Patch)

The issue has been fully resolved in version **1.4.8.6**. The update implements strict validation within the process creation logic. We strongly recommend that all customers update their systems to the latest version as soon as possible.

(Optional Workaround for unpatched systems: Restrict the application server's access to internal IPs and administrative ports at the network/firewall level).

Acknowledgements

We would like to thank **Ianis Bernard from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Hardcoded Cryptographic Keys and Weak IV Generation in linqi

Advisory ID: SEC-2026-001
Publication Date: June 05, 2026
Status: Resolved

Overview

- **CVE-ID:** CVE-2026-11347
- **Vulnerability Type:** Hardcoded Cryptographic Keys (CWE-321), Weak IV Generation (CWE-338)
- **Severity:** High
- **CVSS Base Score:** 8.5

Affected Products

- **linqi** OnPremise – **All versions prior to 1.4.8.6**

Vulnerability Description

A security vulnerability regarding the handling of cryptographic mechanisms has been identified in the affected versions of our application. The software uses hardcoded cryptographic keys for configuration values. Additionally, an algorithm using a weak ASCII character set is employed for the dynamic generation of Initialization Vectors (IVs) for AES/CBC encryption.

Solution (Patch)

The issue has been fully resolved in version **1.4.8.6**. We strongly recommend that all customers update their systems to the latest version as soon as possible.

Acknowledgements

We would like to thank **Ianis Bernard from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: LDAP Injection in linqi

Advisory ID: SEC-2024-001
Release Date: May 14, 2024

Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33868
- **Vulnerability Type:** LDAP Injection (CWE-90)
- **Severity:** Critical
- **CVSS Base Score:** 9.8

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

A security vulnerability in the handling of LDAP queries was discovered in the affected versions of our software. When processing user input on Windows systems, specific LDAP characters are not sufficiently sanitized. This allows a remote attacker to inject malicious LDAP control characters (LDAP Injection).

Solution (Patch)

The issue has been fully resolved in version **1.4.0.1**. We strongly recommend that all customers update their systems to the latest version as soon as possible.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Hardcoded Password Salt in linqi

Advisory ID: SEC-2024-002
Release Date: May 14, 2024
Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33867
- **Vulnerability Type:** Use of Hard-coded Password / Salt (CWE-259)
- **Severity:** Medium
- **CVSS Base Score:** 4.8

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

In versions prior to 1.4.0.1, it was identified that the software uses a hardcoded password salt. A hardcoded cryptographic salt reduces the security of hashed passwords, as attackers with access to the source code or binaries can extract the salt and reuse it for dictionary or rainbow table attacks.

Solution (Patch)

The issue has been fully resolved in version **1.4.0.1**. We recommend a timely update to this version.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Cross-Site Scripting (XSS) in DocumentTemplate API

Advisory ID: SEC-2024-003
Release Date: May 14, 2024
Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33866
- **Vulnerability Type:** Cross-site Scripting / XSS (CWE-79)
- **Severity:** Medium

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

A vulnerability regarding improper neutralization of input during web page generation was found in linqi. The endpoint `/api/DocumentTemplate/{GUID}` is susceptible to Cross-Site Scripting (XSS). This allows an attacker to execute malicious scripts in a victim's browser.

Solution (Patch)

The issue has been fully resolved in version **1.4.0.1**. Please install the corresponding update.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: NTLM Hash Leak via API Endpoints

Advisory ID: SEC-2024-004
Release Date: May 14, 2024
Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33865
- **Vulnerability Type:** Exposure of Sensitive Information (CWE-200)
- **Severity:** High

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

A vulnerability in the endpoints `/api/Cdn/GetFile` and `/api/DocumentTemplate/{GUID}` allows the unauthorized exposure of sensitive information. Through a specifically crafted request, an NTLM hash leak can occur, allowing attackers to intercept the server's NTLM authentication hashes.

Solution (Patch)

The issue has been resolved in version **1.4.0.1**. We recommend an immediate update for all customers.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Server-Side Request Forgery (SSRF) via Document Template Generation

Advisory ID: SEC-2024-005
Release Date: May 14, 2024
Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33864
- **Vulnerability Type:** Server-Side Request Forgery / SSRF
- **Severity:** High

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

An SSRF (Server-Side Request Forgery) vulnerability was discovered in the document template generation process. By embedding remote images during PDF generation via malicious JavaScript, attackers can induce the server to execute server-side requests to

arbitrary internal or external systems. Local file inclusion is also possible through this vector.

Solution (Patch)

The vulnerability was closed with the update to version **1.4.0.1**. Please update the affected systems.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.

Security Advisory: Local File Inclusion in GetFile API

Advisory ID: SEC-2024-006
Release Date: May 14, 2024
Status: Resolved

Overview

- **CVE-ID:** CVE-2024-33863
- **Vulnerability Type:** Local File Inclusion / LFI
- **Severity:** Critical
- **CVSS Base Score:** 9.8

Affected Products

- **linqi** for Windows – **All versions prior to 1.4.0.1**

Description

A critical vulnerability was found in the API endpoint `/api/Cdn/GetFile`. Due to insufficient validation of file paths, a Local File Inclusion (LFI) vulnerability exists. An attacker can exploit this vulnerability to read arbitrary local files from the server's file system, leading to severe information disclosure.

Solution (Patch)

This critical issue was patched in version **1.4.0.1**. We strongly recommend installing the update immediately.

Credits

We would like to thank **Arnoldas Radisauskas from the NATO Cyber Security Centre (NCSC)** for his professional report and cooperation.