

ALTAI TECHNOLOGIES

SECURITY ADVISORY

Name: Potential Security Vulnerabilities in Third-Party Software Components

Advisory ID: ALTAI-SA-2026-001

Publication Date: 26 October 2026

Last Updated: 26 October 2026

Status: Investigation and Remediation in Progress

Overview

Altai Technologies is aware of recently disclosed security vulnerabilities affecting certain third-party software components used in network management platforms. As part of our ongoing cybersecurity monitoring and assessment activities, we have initiated a security review to evaluate the potential impact on Altai products and services.

Our engineering and security teams are actively investigating these vulnerabilities and implementing appropriate remediation measures.

At this time, we have found no evidence of unauthorized access to or compromise of customer data. No immediate customer action is required based on our current assessment.

Affected Products and Components

Component	Potentially Affected Products	Current Status
PHP	AltaiCare on Public & Private Cloud, AltaiCare On-Premises; AltaiGate; AltaiCare Mini;	Security vulnerabilities identified; impact assessment and remediation in progress
Node.js	AltaiCare software platforms; Altai Insights; Partner Portal;	No apparent vulnerabilities identified to date
Java Development Kit (JDK)	AltaiCare software platforms;	Under investigation
Linux	AltaiCare software platforms; Altai Insights; Partner Portal	Under investigation

The inclusion of a product in this advisory does not necessarily indicate that it is exploitable. Product-specific exposure and impact assessments are ongoing.

Remediation Status

Cloud-Based Deployments: For affected Cloud-based deployments, security fixes are expected to be available within one week of this advisory’s publication. Altai will coordinate necessary remediation activities for deployments under its management.

On-Premises and Hardware-Based Deployments: For AltaiCare On-Premises, AltaiGate, and AltaiCare Mini, remediation plans and applicable software updates will be communicated as they become available.

Other Platforms: The potential impact on Partner Portal and Insight is being assessed, and appropriate remediation measures will be implemented where necessary.

Customer Impact and Recommended Actions

- **Customer Data:** No evidence of unauthorized access to or compromise of customer data has been identified.
- **Customer Action:** No immediate action is required from customers at this stage.
- **Service Availability:** Remediation activities are being coordinated to minimize potential service disruption.
- **Further Updates:** Additional information will be provided if our investigation identifies new risks or actions required from customers.

Customers are encouraged to follow Altai’s official security advisories for the latest information.

Ongoing Investigation

Our engineering and security teams continue to assess the potential impact of the identified vulnerabilities, including those associated with JDK and Linux components. We will update this advisory as additional findings become available and remediation measures are finalized.

Contact Information

For questions or concerns regarding this advisory, please contact your Altai representative or Altai Technical Support through our official support channels.

Altai Technologies remains committed to maintaining the security, integrity, and reliability of our products and services.

Revision History

Date	Version	Description
26 October 2026	1.0	Initial security advisory published