ALTAI TECHNOLOGIES

SECURITY ADVISORY

Potential Security Vulnerabilities in Third-Party Software Components

Advisory ID: ALTAI-SA-2026-001

Publication Date: 26 October 2026

Last Updated: 27 October 2026

Version: 1.1

Status: Cloud Remediation Completed; Other Assessments Ongoing

Overview

Altai Technologies has reviewed recently disclosed security vulnerabilities affecting third-party software components used in certain network management platforms. Our engineering and security teams have implemented security updates for the assessed cloud-hosted PHP environments and continue evaluating potential impacts on other products and components.

Based on our investigation to date, 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	Products / Services Under Review	Current Status
PHP	AltaiCare on Public & Private Cloud; AltaiCare On-Premises; AltaiGate; AltaiCare Mini;	Cloud-hosted PHP environments assessed and updated; remaining product-specific assessments and remediation planning continue.
Node.js	AltaiCare software platforms; Altai Insights; Partner Portal	No apparent vulnerabilities identified to date.
JDK	AltaiCare software platforms	Under investigation.
Linux	AltaiCare software platforms; Altai Insights and Partner Portal	Under investigation.

Listing a product or service does not mean it has been confirmed exploitable. Exposure and remediation status may differ by deployment.

Identified CVEs and Remediation

For the assessed cloud-hosted PHP environments, Altai upgraded PHP runtimes to supported versions and applied additional security configurations. Systems were upgraded to PHP 8.5.12 or PHP 8.3.36, as appropriate. These updates addressed CVE-2026-109618 and CVE-2026-109619 in the assessed environments.

Additional security controls were implemented to further reduce potential exposure associated with CVE-2026-111497.

CVE ID	Affected Component	Result
CVE-2026-109618	Portal Services	Resolved
CVE-2026-109619	Portal Services	Resolved
CVE-2026-111497	Portal Services	Security Enhancements Applied

Remediation Status

Cloud-Based Deployments: Security updates for the assessed Altai-managed cloud-hosted PHP environments were completed on 27 October 2026. Altai continues to verify applicability and coverage across relevant services.

On-Premises and Hardware-Based Deployments: Assessment and remediation planning for AltaiCare On-Premises, AltaiGate and AltaiCare Mini remain ongoing. Applicable software updates or further guidance will be communicated when available.

Customer Impact and Recommended Actions

- Customer Data: No evidence of unauthorized access to or compromise of customer data has been identified to date.
- Customer Action: No immediate customer action is required based on the current assessment.
- Further Updates: Altai will update this advisory if additional risks, affected deployments, or required customer actions are identified.

Ongoing Investigation

Our engineering and security teams continue assessing the applicability of JDK and Linux vulnerabilities and any outstanding product-specific exposure. This advisory will be updated as findings are confirmed and remediation progresses.

Contact Information

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

Revision History

Date	Version	Description
26 October 2026	1.0	Initial security advisory published.
27 October 2026	1.1	Updated PHP vulnerability findings, cloud-hosted remediation status, PHP runtime upgrade details, and CVE remediation results for assessed portal services.

© 2026 Altai Technologies Ltd. All rights reserved.