Subject: aPriori Response to the PHP Security Vulnerabilities
Date: October 22, 2026

Customers have asked whether aPriori is affected by the recently disclosed PHP vulnerabilities (CVE-2026-109618 and CVE-2026-109619). This notice explains where we stand.

Summary
aPriori has reviewed its environments for exposure. The only potentially affected systems we identified were our public websites, and they have already been patched.

aPriori Company Website (apriori.com)
The content-only sites are hosted on a separate and isolated platform operated by our partner, Kinsta. Kinsta has confirmed deployment of patches across its platform, and aPriori has verified that our WordPress environments include fixes for both vulnerabilities. No customer action is required. (https://status.kinsta.com/incidents/c0c6xl1ghpb2)

aPriori Cloud Software
aPriori Cloud software does not use PHP and is not affected by these vulnerabilities. No customer action is required.

aPriori On-Premise Software
aPriori On-Premise software does not include or depend on PHP. Customers should still follow their own organization's patching process for any PHP installations in their environments that are unrelated to aPriori.

aPriori Auxiliary Applications (plugins, agents, and so on)
None of aPriori's plugins, agents, or other auxiliary applications use PHP and none are affected. Customers should still follow their own organization's patching process for any PHP installations in their environments that are unrelated to aPriori.

aPriori Corporate Systems
aPriori has confirmed that no aPriori corporate systems are affected.

Questions
If you have questions, please contact aPriori Support at support@apriori.com. We will update this notice if anything changes.