scrive.

Security communique

PHP2Shell vulnerability and Scrive services

Issued 3 November 2026 · Version 1.0 · Scrive Security Office

Scrive's core services are not affected by the PHP2Shell vulnerabilities, because they do not use PHP. The few Scrive components that do use PHP have been patched, and we have seen no indication of exploitation. No action is required from Scrive customers or partners.

This communique is issued so that customers and partners can reference Scrive's official position in their own vulnerability assessments. It covers Scrive eSign (including Scrive GO, Forms and APIs), Contractbook and esignatur.

About the vulnerability

PHP2Shell is the name given to two critical flaws in the PHP runtime itself: CVE-2026-109618 and CVE-2026-109619. On an unpatched system an unauthenticated attacker can run code on the server. Both are rated CVSS 9.2, and the PHP project published fixes on 21 October 2026.

Exploitation has been observed in the wild and the CVEs are on CISA's Known Exploited Vulnerabilities list. Patching to a fixed release (PHP 8.2.35, 8.3.36, 8.4.27 or 8.5.12) is the only complete fix.

Impact on Scrive services

None of Scrive's core signing, sign-in or API services use PHP, so neither CVE applies to them. PHP exists at Scrive only in two customer-specific integrations and in the public marketing websites, all of which are hosted separately from the production platform and have been patched. We have no indication that any customer data held in Scrive, Contractbook or esignatur was accessed.

Service or component	Uses PHP	Affected	Status
Scrive eSign (Standard and EC), incl. Scrive GO, Scrive GO POS, Forms, Forms Builder, APIs and	No	Not affected	No action needed

hosted platform components			
esignatur	No	Not affected	No action needed
Contractbook	No	Not affected	No action needed
Two customer-specific integrations (each used by a single customer, run outside the core production environment)	Yes	Vulnerable until patched	Patched to a fixed PHP release on 22 October 2026, verified by version check
Public marketing websites for Scrive and esignatur (WordPress, hosted by our web agency)	Yes	Vulnerable until patched	Taken offline 21 October 2026 for roughly five hours while the fix was installed; now on PHP 8.3.36, the fixed release

The marketing websites are content sites only. They are separate from the Scrive product, the sign-in flow and the signing services, and the login link remained available on the error page throughout the maintenance window. The two integrations were already isolated from the core production infrastructure before patching, so an attack against them could not have reached the platform or customer documents.

What Scrive has done

All PHP components were patched within roughly 24 hours of the fixes being released, and the remediation is complete. The Security Office and Infrastructure Operations team acted as follows:

1. 21 October 2026, morning: inventory of every PHP workload in Scrive's infrastructure opened as a P0 ticket before the PHP fixes were published, identifying the integrations and the public websites.
2. 21 October 2026, afternoon: the marketing websites were taken offline as a precaution until the fixed PHP release could be installed, then updated and brought back online the same evening.
3. 22 October 2026: new builds of the affected integrations with the fixed PHP runtime were deployed to production, and the fix was verified by version check. A further runtime bugfix build was rolled out on 26 October 2026.
4. Monitoring: our security monitoring has shown no indication of exploitation attempts against Scrive's infrastructure, and no sign of compromise, before or after patching.
5. Hardening: automated dependency updates have been enabled for the remaining PHP integrations so future runtime fixes are picked up promptly, and most such bespoke integrations have already been re-implemented in Scrive's main codebase or phased out.

No temporary protective measures remain in place; the isolation of the integrations from the core production environment was already permanent before this event.

What customers and partners need to do

Nothing. No action is required from Scrive, Contractbook or esignatur customers, partners or their end users, and no credentials, API keys or integrations need to be rotated or changed.

For your own vulnerability assessment, you are welcome to reference the following statement:

> Scrive confirms that its core services are not affected by CVE-2026-109618 or CVE-2026-109619, as they do not use PHP. All Scrive components that do use PHP have been updated to address these vulnerabilities. We have seen no indication of exploitation.

Third-party services that you use together with Scrive, such as identity verification or eID providers, are covered by those providers' own advisories, and we recommend you consult them directly where your assessment requires it.

Should our assessment change, we will update this communique and notify affected customers directly.

Contact

Questions about this communique or requests for further detail to support a security assessment can be sent to the Scrive Security Office via your Scrive, Contractbook or esignatur contact, or through Scrive Support.

Juris Puce
CISO, Scrive AB

This document reflects Scrive's assessment as of the issue date. Public references: Pentest-Tools PHP2Shell research (pentest-tools.com/research/php2shell-rce), CERT-SE advisory (cert.se), CERT-EU advisory 2026-018 (cert.europa.eu).