Teknisk post mortem

Kritisk PHP-sårbarhet – CVE-2026-109618 / CVE-2026-109619

Status: Slutlig **Klassificering:** Publik **Datum:** 2026-10-22
Ägare: Robin Alm, CTO – Askås *Tider i lokal tid (Europe/Stockholm, UTC+2), UTC inom parentes där relevant.*

Sammanfattning

Två kritiska sårbarheter i PHP-kärnan (CVSS 9.2, oautentiserad RCE) offentliggjordes 21 oktober 2026. Askås agerade proaktivt redan på förhandsvarningen, och genom automatiserad utrullning var majoriteten av servrarna patchade inom 1 timme efter att rättningen släpptes och samtliga inom ca 2 timmar. Eskaleringsrutinerna fungerade enligt plan. Loggning har inte visat några tecken på utnyttjande i vår miljö.

1. Sårbarhet

	CVE-2026-109618	CVE-2026-109619
Komponent	Multipart/form-data-parsern (PHP-kärna)	session.upload_progress-hanteraren
Typ	Minneskorruption → RCE	Minneskorruption (UAF) → RCE
Vektor	Oautentiserad HTTP POST mot vilken körbar PHP-endpoint som helst	Multipart-POST med fältet PHP_SESSION_UPLOAD_PROGRESS + aktiv session
CVSS v4.0	9.2	9.2

Viktig teknisk konsekvens: Sårbarheten ligger i tolkens request-hantering, före att applikationskoden körs. Det krävdes därför i princip inget av vår PHP-kod för att vara exponerad – en oautentiserad POST mot en nåbar .php räckte. Mängden egen PHP-kod påverkade inte exponeringen, bara antalet publikt nåbara PHP-endpoints.

Patch var enda fullständiga åtgärden. Config-baserade mitigeringar (t.ex. session.upload_progress.enabled=Off) adresserar endast -109619, inte multipart-vektorn i -109618. Detta bekräftades av flera externa källor (Datadog, AWS, Prophet).

Fixade versioner: 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12, samt backports för 7.4/8.0/8.1 via deb.sury.org.

2. Tidslinje

Tidpunkt (lokal / UTC)	Händelse
17 okt	(Externt, känt i efterhand) AWS MadPot registrerar första utnyttjandeförsöket mot honeypot – fyra dagar före publik disclosure.
Tis 20 okt, em	Förhandsvarning om kommande PHP-säkerhetspatch. Intern bevakning inleds.
Ons 21 okt, 02:00 UTC	(Externt) Tidigaste PoC:er dyker upp, före embargots slut.
Ons 21 okt, fm	Rykten om tekniska detaljer sprids. Riskbedömning påbörjas.
Ons 21 okt, ~13:20	**BESLUT** att uppdatera miljöer med äldre PHP (7.x, 8.2.x). Förberedande uppdatering mot 8.5 – osäkert vilka grenar som skulle få patch.
Ons 21 okt, 14:31	Information om förberedande arbete publiceras på status.askas.com.
Ons 21 okt em	Känt att deb.sury.org även släpper patchade 7.x/8.2.x. Arbetet fokuseras på Sury-repot för servrar som krävde högre version än OS:ets ordinarie repo.
Ons 21 okt, 16:00 (14:00 UTC)	OFFICIELL PATCH SLÄPPS. Automatiserad utrullning startar. Flera servrar patchade inom minuter.
Ons 21 okt, ~17:00	Majoriteten av servrarna patchade (inom ~1 h).

Tidpunkt (lokal / UTC)	Händelse
Ons 21 okt, ~18:15	Samtliga servrar patchade (ca 2 timmar efter release).
Ons 21 okt, efter 14:00 UTC	(Externt) Bred exploatering “in the wild” enligt AWS.

> **Notering: Den stegvisa utrullningen av** patch sker automatiserat och rullas ut i omgångar – det är förklaringen till att servrarna inte patchas exakt samtidigt. Detta är avsiktligt (kontrollerad utrullning), inte en fördröjning. Resultatet – majoritet <1 h, alla <2 h – ligger i linje med branschrekommendationen att mäta patchtid för kritiska internetexponerade sårbarheter i timmar, inte dagar.

3. Exponeringsfönstret

AWS MadPot observerade utnyttjandeförsök redan 17 oktober, före disclosure. Det innebär att det fanns ett branschgemensamt exponeringsfönster som föregick patchen och som ingen försvarares patchhastighet kunde ha eliminerat. Tiden från patch-release till applicerad patch (~2 h hos oss) är därför en liten del av den totala riskbilden – den reella exponeringen definierades av att sårbarheten var publik och utnyttjad innan en rättning överhuvudtaget fanns.

Slutsatsen är att snabb patchning var rätt och väl utförd, men att ”noll exponering” aldrig var uppnåeligt för någon aktör i detta fall. Det förstärker värdet av de kompletterande kontrollerna (detektion, loggning, isolering) snarare än enbart patchhastighet.

4. Q&A

Blev vi utnyttjade?
Ingen indikation på det i tillgänglig loggning.

Varför patchades inte alla servrar samtidigt?
Patchningen är automatiserad och rullas ut i kontrollerade omgångar. Majoritet <1 h, alla <2 h.

Räckte det inte att slå av session.upload_progress?
Nej. Det adresserar bara CVE-2026-109619. Huvudsårbarheten (CVE-2026-109618) sitter i multipart-parsern och åtgärdas endast av patch.

Spelar det någon roll att uppdateringen genomfördes snabbt när försök hade observerats redan den 17 oktober?

Ja. En snabb uppdatering begränsade exponeringsfönstret efter att säkerhetspatchen blev tillgänglig. Samtliga berörda servrar uppdaterades inom cirka två timmar.

5. Övrigt

På en server där inga e-handelsapplikationer hostas, så kördes php medvetet i en lägre version för vissa kunder. Där har nu äldre versioner inaktiverats vilket gör att applikationer som inte uppdaterats nyligen kan ha kompatibilitetsproblem. Om du som kund upptäcker att funktioner slutat fungera, kontakta Askås för hjälp.