



Številka: 386-62/2026-1544-1

Datum: 21. 10. 2026

Na podlagi prvega in petega odstavka 37. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1) Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) kot pristojni nacionalni organ iz prvega odstavka 10. člena ZInfV-1 zaradi kritične ranljivosti v programskem jeziku PHP (CVE-2026-109618 in CVE-2026-109619), posodablja oceno ogroženosti kibernetске varnosti v Republiki Sloveniji in podaja oceno, da je ogroženost varnosti omrežij in informacijskih sistemov zavezancev po ZInfV-1 ovrednotena kot visoka ogroženost. Visoka ogroženost se nanaša tudi na druge organe in organizacije, ki uporabljajo programski jezik PHP ali programsko opremo, ki PHP vsebuje oziroma je od njega odvisna.

Ocena visoke ogroženosti velja do preklica. Zavezanci morajo v skladu s petim odstavkom 37. člena ZInfV-1 nemudoma začeti izvajati predpisane dodatne varnostne ukrepe in jih izvajati do preklica.

Obrazložitev:

URSIV je na podlagi objavljenih analiz in pridobljenih informacij ter v sodelovanju z drugimi pristojnimi organi in organizacijami ugotovil, da je prišlo do odkritja ranljivosti, ki bi lahko resno vplivala na varnost informacijskih sistemov ter omrežij zavezancev in širše, kar bi lahko vplivalo na spremembo varnostnih razmer. Omenjeno stanje zahteva posodobitev ocene ogroženosti iz prvega odstavka 37. člena ZInfV-1. Resno je ogrožena varnost omrežij in informacijskih sistemov zavezancev po ZInfV-1 in tudi drugih organizacij, ki uporabljajo programski jezik PHP. PHP je eden najbolj razširjenih strežniških skriptnih jezikov za razvoj spletnih aplikacij in je podlaga številnim sistemom za upravljanje vsebin, spletnim portalom in drugim rešitvam v široki uporabi v javnem in zasebnem sektorju, kar bi lahko imelo velik vpliv na centralni državni informacijsko-komunikacijski sistem, organizacije javnega sektorja in širše.

Razvijalci PHP so 20. oktobra 2026 napovedali izdajo varnostnih popravkov in si pridržali pravico do zgodnejše izdaje, če bi podrobnosti ranljivosti postale javne ali če bi se pokazalo izkoriščanje. Po navedbah posameznih varnostnih ponudnikov so podrobnosti pred načrtovanim usklajenim razkritjem odtele v javnost, česar PHP v svoji objavi ne navaja. Popravke so izdali 21. oktobra 2026 v različicah PHP 8.2.35, 8.3.36, 8.4.27 in 8.5.12. Odpravljajo dve kritični ranljivosti z oznakama CVE-2026-109618 in CVE-2026-109619, obe ocenjeni z oceno CVSS v4.0 9,2 od 10. Ranljive so vse različice PHP pred navedenimi, vključno s tistimi, ki jim je podpora potekla. Za PHP 8.1 in starejše rednih izdaj ni več, je pa varnostna ekipa PHP zaradi resnosti objavila minimalne izvirne popravke za PHP 7.4, 8.0 in 8.1, popravljene pakete pa pripravljajo tudi distribucije in ponudniki podaljšane podpore, zato naj se uporabniki obrnejo na svojega ponudnika. Opozarjamo tudi, da je PHP 8.2 ob koncu podpore 31. decembra 2026, kar je treba upoštevati pri načrtovanju nadgradenj.

Ranljivosti omogočata oddaljeno izvajanje poljubne kode brez predhodne avtentikacije, in sicer s pravicami procesa spletnega strežnika. Ranljivost CVE-2026-109618 izhaja iz neustrezne obravnave pomanjkanja pomnilnika (OOM), zaradi katere PHP pri zaključevanju zahteve obdela le delno inicializirane podatke. Ranljivost CVE-2026-109619 izhaja iz notranjega stanja, ki po zaključku zahteve

ostane v delovnem procesu in ga lahko naslednja zahteva uporabi po sprostitvi pomnilnika. Izkoriščanje je bilo potrjeno na izvedbi Apache mod_php, pri ranljivosti CVE-2026-109619 tudi na PHP-FPM, pri čemer potrjena izvedljivost na teh dveh izvedbah ne pomeni, da druge niso izpostavljene. Po navedbah projekta je ogrožena vsaka namestitev, ki streže spletne zahteve, vključno s PHP-FPM, Apache z mod_php, php-cgi, FrankenPHP in LiteSpeed, najvišje tveganje pa je pri mod_php, kjer se napad sproži še pred izvedbo aplikacijske kode.

Posamezni varnostni ponudniki so 21. oktobra 2026 poročali o prvih poskusih izkoriščanja, drugi tega pri svojih strankah niso zaznali, PHP izkoriščanja ni potrdil, ranljivosti pa tudi še nista uvrščeni na seznam aktivno izkoriščanih ranljivosti CISA. Pojavljajo se tudi navedbe o odtekli kodi za izkoriščanje, ki je nismo neodvisno potrdili. Namestitev popravkov je edini popoln ukrep, začasni konfiguracijski ukrepi tveganje le zmanjšajo.

Za CVE-2026-109618 nastavitev `memory_limit=-1`, po možnosti prek `php_admin_value` v nastavitvi sklada FPM ali strežnika Apache, ob tem pa omejitev pomnilnika na ravni vsebnika ali cgroup, po možnosti tako, da se ob prekoračitvi prekine le prizadeti delovni proces. Omejitev `RLIMIT_AS` in `RLIMIT_DATA` se ne uporablja, ker ob dosegu meje sproži prav ranljivo izvajalno pot. Poleg tega nizka vrednost `post_max_size` in `upload_max_filesize` pod njo ter omejevanje velikosti zahtev na strežniku ali posredniku.

Pri programski opremi z vgrajeno različico PHP posodobitve pripravi njen proizvajalec. Priporočamo, da se od proizvajalca zahteva rok za izdajo popravka, do takrat pa se uveljavijo zgoraj navedeni začasni ukrepi in omeji izpostavljenost prizadete storitve iz interneta.

Na podlagi devetega odstavka 37. člena ZInFV-1 bo URSIV za zmanjšanje visoke ogroženosti ter preprečitev nastanka krize oziroma njeno obvladovanje izdal pisno odredbo, s katero bo zavezancem odredil izvedbo nujnih ukrepov in jih s tem seznanil. URSIV bo nadaljnje dogajanje pozorno spremljal ter po potrebi nemudoma sprejel dodatne sorazmerne ukrepe in o njih po potrebi obvestil tudi širšo javnost.

dr. Niko Gamulin

v. d. direktorja urada