



Številka: 386-62/2026-1544-2

Datum: 21. 10. 2026

Na podlagi devetega odstavka 37. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljnjem besedilu: ZInfV-1) in ocene ogroženosti št. 386-62/2026-1544-1 z dne 21. 10. 2026, s katero je bila ugotovljena visoka ogroženost, Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu: URSIV) kot pristojni nacionalni organ iz prvega odstavka 10. člena ZInfV-1 izdaja naslednjo

ODREDBO

o izvedbi nujnih ukrepov v zvezi s kritičnima ranljivostma CVE-2026-109618 in CVE-2026-109619 v programskem jeziku PHP

Za nižanje ocene visoke ogroženosti ter posledično preprečitev nastanka krize se odreja izvedba nujnih ukrepov pri zavezancih (v nadaljnjem besedilu: naslovniki). S to odredbo se določajo vrsta in obseg del, ki jih je treba opraviti pri navedenih subjektih, ter roki za njihovo izvedbo.

Nujni ukrepi

I. Identifikacija

Naslovniki identificirajo vse aplikacije ter omrežne in informacijske sisteme, ki temeljijo na PHP. Prednostno identificirajo aplikacije in sisteme, dostopne prek interneta. Preverijo tudi aplikacije in rešitve, ki uporabljajo vgrajeno različico PHP oziroma so odvisne od PHP, ki ga vzdržuje proizvajalec druge programske opreme.

Rok za izvedbo: 24 ur od seznaitve s to odredbo.

II. Namestitev popravkov

Naslovniki namestijo PHP v različici 8.2.35, 8.3.36, 8.4.27, 8.5.12 ali novejši oziroma posodobljene pakete svojega distributerja ali proizvajalca, ki odpravljajo obe ranljivosti. Pri aplikacijah, ki uporabljajo vgrajeno različico PHP ali različico, ki jo vzdržuje drug proizvajalec, se naslovniki pripravijo na namestitev posodobitve tega proizvajalca in od njega zahtevajo rok za njeno izdajo. Posodobitev namestijo takoj, ko je na voljo.

Po namestitvi naslovniki ponovno zaženejo vse delovne procese PHP in preverijo uspešnost namestitve.

Rok za izvedbo: 48 ur od seznaitve s to odredbo za aplikacije in sisteme, dostopne prek interneta, in 7 dni od seznaitve za druge aplikacije in sisteme. Za posodobitve drugih proizvajalcev rok začne teči z dnem, ko je posodobitev na voljo.

III. Ukrepi, kadar takojšnja namestitvev popravkov ni mogoča

Kadar takojšnja namestitvev popravkov ni mogoča, naslovniki nemudoma ocenijo tveganje in uvedejo ustrezne zaščitne ukrepe, ki tveganje zmanjšajo. Pri tem upoštevajo navodila varnostne skupine PHP:

- memory_limit nastavijo na -1, in sicer tako, da ga aplikacija ne more prepisati (na primer php_admin_value v konfiguraciji sklada FPM ali strežnika Apache). Preverijo, da nobena nastavitvev sklada, imenika ali aplikacije ne vzpostavi ponovno končne omejitve. Zaradi ohranitve razpoložljivosti uvedejo omejitev pomnilnika na ravni vsebnika ali cgroup, po možnosti tako, da se ob prekoračitvi prekine le prizadeti delovni proces, pri čemer ta omejitev ne prepreči nujno neuspele dodelitve pomnilnika. Omejitev RLIMIT_AS in RLIMIT_DATA ne uporabljajo.
- post_max_size nastavijo na nizko vrednost: 8M, če aplikacija ne potrebuje nalaganja datotek, oziroma 32M, če ga potrebuje. Vrednost upload_max_filesize mora biti nižja od vrednosti post_max_size. Na spletnem strežniku ali posredniku omejijo velikost dekodirane zahteve, število vhodnih polj, število delov multipart, število glav na posamezen del, število nalaganj in globino gnezdenja (max_input_nesting_level).
- Če aplikacija zahtev multipart ne uporablja, jih na spletnem strežniku ali posredniku zavrnejo.
- session.upload_progress.enabled nastavijo na 0 v php.ini, v konfiguraciji sklada FPM ali v konfiguraciji strežnika, ki se uveljavi pred razčlenjevanjem zahteve. Nastavitvev s funkcijo ini_set() ali v datoteki .user.ini ne zadošča.
- Pri PHP 8.5 nastavijo fatal_error_backtraces na 0.
- Odstranijo neveljavne ali zastarele nastavitve, ki se uveljavljajo za posamezno zahtevo in sprožajo diagnostična sporočila pred inicializacijo. Prikrivanje diagnostike z error_reporting, display_errors ali @ ne zadošča.
- Odpravijo zlonamernemu akterju dosegljive usodne napake in prekoračitve časa izvajanja, ker prav te sprožijo CVE-2026-109619.
- Pri skladih FPM, kadar zmogljivost to dopušča, nastavijo pm.max_requests na 1.
- Po spremembah nastavitvev ponovno zaženejo vse delovne procese PHP.

Če ukrepov iz te točke ni mogoče izvesti ali ne zadošča, naslovniki do namestitvev popravkov začasno omejijo dostop do izpostavljenih aplikacij oziroma jih izolirajo od javnih omrežij.

Ukrepi iz te točke ne nadomeščajo namestitvev popravkov.

IV. Različice brez podpore

Za sisteme s PHP 8.1 ali starejšim naslovniki namestijo popravke, ki jih zagotavlja distributer ali ponudnik podaljšane podpore, oziroma minimalne popravke izvirne kode, ki jih je za različice 7.4, 8.0 in 8.1 objavila varnostna skupina PHP. Sicer sisteme nadgradijo na podprto različico. Do izvedbe ukrepa sisteme izolirajo od javnih omrežij.

Rok za izvedbo: enak kot v II. točki.

V. Spremljanje in preverjanje znakov izkoriščanja

Naslovniki spremljajo uradna varnostna obvestila projekta PHP, proizvajalcev programske opreme in pristojne skupine CSIRT. Pri sistemih, ki ob objavi popravkov niso bili posodobljeni, preverijo morebitne znake poskusov izkoriščanja ali kompromitacije, zlasti:

- usodne napake zaradi prekoračitve pomnilnika (dnevniški zapis "Fatal error"), posebej pri zahtevah multipart,
- sesutja in nepričakovane izhode delovnih procesov PHP-FPM ali spletnega strežnika,
- nepričakovane procese ali datoteke pod uporabniškim računom spletnega strežnika in
- prisotnost spletnih lupin ali drugih zadnjih vrat.

Ob tem zagotovijo ohranitev dnevniških zapisov in jih zavarujejo pred prepisom.

VI. Priglasitev incidentov

Zaznane pomembne incidente naslovniki prigrasijo pristojni skupini CSIRT v skladu s 30. členom ZInfV-1. Zavezanci, ki niso bistveni ali pomembni subjekti, lahko zaznavo sporočijo s prostovoljno prigrasitvijo po 35. členu ZInfV-1.

VII. Poročanje

O izvedbi ukrepov iz I. do V. točke naslovniki poročajo pristojni skupini CSIRT na način, ki ga določi njeno varnostno navodilo. Če varnostno navodilo ni izdano, naslovniki poročajo na naslov in v obliki, kot ju določa ta odredba.

Rok za izvedbo: 72 ur od seznaitve s to odredbo, nato ob vsaki spremembi stanja do izvedbe vseh ukrepov.

Obrazložitev:

URSIV je zaradi nenadne spremembe varnostnih razmer, povezane s kritičnima ranljivostma v programskem jeziku PHP (CVE-2026-109618 in CVE-2026-109619), z dokumentom št. 386-62/2026-1544-1 z dne 21. 10. 2026 posodobil oceno ogroženosti kibernetike varnosti v Republiki Sloveniji in ogroženost varnosti omrežij in informacijskih sistemov zavezancev po ZInfV-1 ovrednotil kot visoko.

Navedeni ranljivosti je varnostna skupina PHP ocenila kot kritični, z oceno CVSS v4.0 9,2 od 10, saj lahko omogočita oddaljeno izvajanje poljubne kode brez predhodne avtentikacije, in sicer s pravicami procesa spletnega strežnika. V oceni je navedeno, da se visoka ogroženost nanaša tudi na druge organe in organizacije, ki uporabljajo programski jezik PHP ali programsko opremo, ki PHP vsebuje oziroma je od njega odvisna.

Tehnična zahtevnost možnih zlonamernih aktivnosti in potrebni pogoji sta v oceni CVSS (vektor CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N) ovrednotena kot zahtevnejša, zato nujnost ukrepov ne izhaja le iz ocene CVSS. Izhaja predvsem iz potrjene izvedljivosti izkoriščanja ranljivosti. Varnostna skupina PHP navaja, da je bilo popolno oddaljeno izvajanje kode prek protokola HTTP potrjeno pri izvedbi Apache mod_php s privzetimi omejitvami vhoda in pomnilnika, pri čemer se izkoriščanje ranljivosti sproži še pred izvedbo aplikacijske kode. Pri ranljivosti CVE-2026-109619 je bilo izvajanje kode potrjeno tudi pri PHP-FPM, prek funkcije spremljanja napredka nalaganja sej, ki je privzeto omogočena.

Varnostna skupina PHP je izdajo popravkov napovedala 20. 10. 2026 in si pridržala 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 varnostna skupina PHP v svojih objavah ne navaja. Popravke je izdala 21. 10. 2026 v različicah 8.2.35, 8.3.36, 8.4.27 in 8.5.12. Po njenih navedbah so ranljive vse različice pred navedenimi, vključno s tistimi, ki jim je podpora potekla; za PHP 7.4, 8.0 in 8.1 je zaradi resnosti objavila minimalne popravke izvirne kode, rednih izdaj za te različice pa ni. Ogrožene so vse namestitve PHP, ki strežejo spletne zahteve, največje tveganje pa je pri izvedbi Apache mod_php. Namestitev popravkov je po njenih navedbah edini popoln ukrep, začasni ukrepi pa zmanjšajo izpostavljenost le posameznim načinom izkoriščanja ranljivosti.

Ob izdaji popravkov so posamezni varnostni ponudniki poročali o prvih poskusih izkoriščanja, drugi jih niso zaznali, varnostna skupina PHP pa izkoriščanja ni potrdila. Ker so bile po navedbah varnostnih ponudnikov podrobnosti ranljivosti javno dostopne že pred izdajo popravkov, URSIV ocenjuje, da je izkoriščanje nepopravljenih sistemov verjetno, ne glede na to, ali je bilo potrjeno.

PHP je eden najbolj razširjenih strežniških skriptnih jezikov in je podlaga številnim spletnim aplikacijam v javnem in zasebnem sektorju. Po telemetriji Cortex Xpanse družbe Palo Alto Networks (Unit 42) z dne 21. 10. 2026 je bilo na internetu zaznanih več kot 22,6 milijona javno dostopnih instanc, potencialno ranljivih za obe ranljivosti. Po pregledu zunanje izpostavljenosti, ki ga je SIGOV-CERT opravil 21. 10.

2026, je bilo v Republiki Sloveniji med javno dostopnimi storitvami, ki razkrivajo različico PHP, zaznanih 1.320 gostiteljev, od tega 316 v podprtih vejah pod mejo popravka (8.2, 8.3, 8.4 in 8.5) in 1.004 v različicah brez podpore. Pregled zajame le storitve, ki različico razkrijejo navzven, zato je dejanska izpostavljenost lahko višja.

Pri programski opremi z vgrajeno različico PHP je odprava ranljivosti odvisna od posodobitev njenih proizvajalcev.

Navedene okoliščine, zlasti kritičnost ranljivosti, možnost njunega izkoriščanja brez predhodne avtentikacije, široka razširjenost PHP ter dejstvo, da začasni ukrepi ne zagotavljajo popolne odprave ranljivosti, utemeljujejo nujnost izdaje odredbe za nižanje ocene visoke ogroženosti in posledično preprečitev nastanka krize.

Glede na navedeno URSIV na podlagi devetega odstavka 37. člena ZInfV-1 s to odredbo odreja izvedbo nujnih ukrepov, pri čemer določa vrsto in obseg del, ki jih je treba opraviti, ter roke za njihovo izvedbo. Odrejeni nujni ukrepi so glede na ugotovljeno visoko ogroženost, resnost in možnost izkoriščanja ranljivosti ter morebitne škodljive posledice za varnost omrežij in informacijskih sistemov potrebni in sorazmerni za doseg namena odredbe.

dr. Niko Gamulin

v. d. direktorja urada