

Kas Interneti vundament kõigub? PHP kriitilised turvaaugud sunnivad veebiteenuseid ajutiselt sulguma

2 tundi tagasi - 21.10.2026 Autor: [AM](#)

Kui oled viimastel tundidel märganud, et mõni suurem veebileht tõrgub või teatab hooldustöödest, pole tegemist juhusega. Veebimaailmas on vallandunud häireolukord: maailma populaarseima "veebikeele" PHP koodist lekkisid kaks kriitilist turvaauku, mille parandamisel käib nüüd võidujooks ajaga. Kuna info turvanõrkuste kohta jõudis hakerite foorumitesse enne ametlikke paikamispakette, on ründajad juba asunud haavatavaid servereid internetiavarustest kokku kammima.

See mure puudutab peaaegu igaüht meist, kellel veebis midagi suuremat üleval. PHP on veebimaailmas nagu tsentraalne veevärk kortermajas. Suur osa tänapäeva internetist, alates WordPressi sisuhaldussüsteemidest kuni kohalike e-poodideni, toetub just sellele mootorile.

Mis täpsemalt juhtus ja miks häirekella lüüakse?

Kõik sai alguse ootamatust infolekkest platvormil [Hacker News](#), kus kasutaja nimega "petecooper" avaldas teate kahe üliohtliku turvaaugu kohta, mida tähistatakse koodidega [CVE-2026-109618](#) ja [CVE-2026-109619](#). Mõlemad vead võimaldavad koodi kaugkäivitust (RCE ehk *Remote Code Execution*), mis tähendab maakeeli seda, et kurikael võib serveri ukse virtuaalselt jalaga lahti lüüa ja masina täielikult enda kontrolli alla võtta, ilma et tal oleks selleks vaja mingeid paroole.

Küberturbeettevõtte watchTowr tegevjuht Benjamin Harris kinnitas väljaandele [BleepingComputer](#), et tegemist pole valehäirega:

"Viimase tunni jooksul on lekkinud kaks PHP koodi kaugkäivituse turvanõrkust. Need olid varem embargoga kaitstud ja pidid avalikuks saama alles neljapäeval kell 11.00 ET. Kuigi me ei saa tundlikkuse tõttu praegu tehnilisi üksikasju jagada, võime kinnitada, et need nõrkused on tõepoolest reaalsed. Mõlema ohuhinnang on CVSS 10 ja meie teada

puudutavad need PHP versioone 5, 6, 7 ja 8."

Ametlik PHP arendusmeeskond hindas vigade raskusastmeks CVSS v4.0 skaalal ülikõrged 9,2 punkti kümnest ning teatas, et erakorralised turvapaigad tehakse kättesaadavaks kolmapäeval, 21. oktoobril kell 14.00 UTC (Eesti aja järgi kell 17.00). PHP tiim manitses administraatoreid:

"Jätame endale õiguse paikade varasemaks avaldamiseks, kui kummagi haavatavuse üksikasjad peaksid avalikuks tulema või kui ilmneb tõendeid nende aktiivsest ärakasutamisest."

Kuidas reageerivad Eesti teenusepakkujad ja CERT-EE?

Olukorra tõsidust on kinnitanud ka Riigi Infosüsteemi Ameti küberintsidentide lahendamise osakond CERT-EE, kes edastas kodumaistele administraatoritele ja asutustele kiire ohuhinnangu. Ohu neutraliseerimiseks hakkasid mitmed kohalikud teenusepakkujad kohe tegutsema: näiteks Veebimajutus.ee ja teised serverite haldajad lükkasid oma teenindavad süsteemid alates kella 17.00-st hooldusrežiimi, et värsked turvapaigad serveripargile viivitamatult peale kanda. [Zone](#) hoiatab võimalike teenusekatkestuste eest seoses PHP uuendustega.

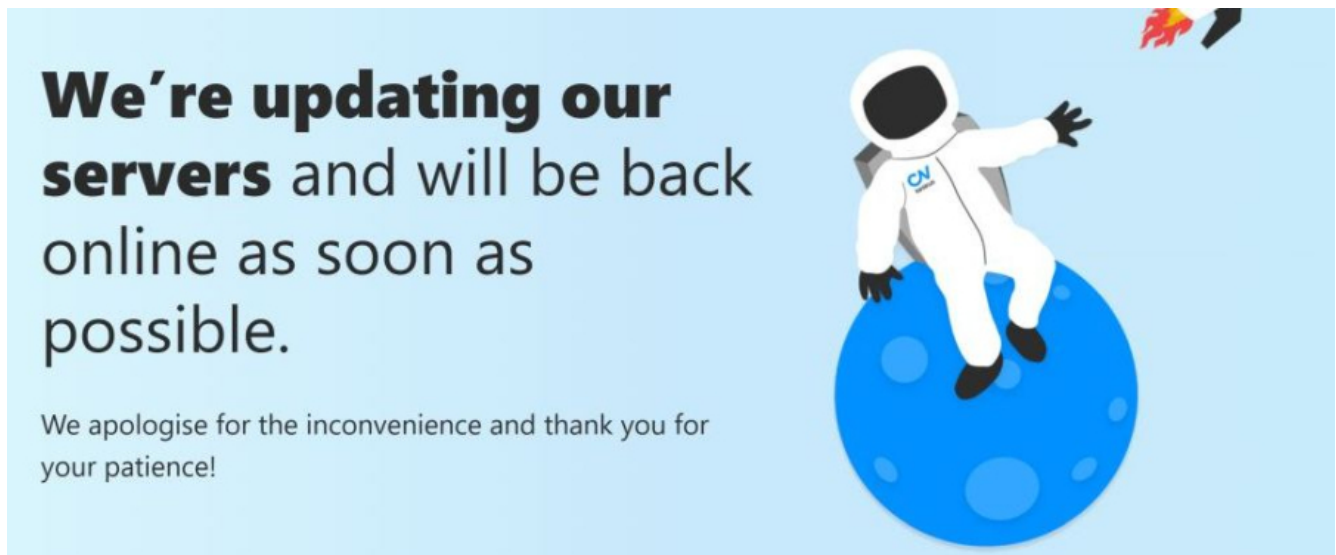


Kuna ründelaine võis alata praktiliselt kohe pärast koodinäidete lekkimist, mida kübermaailmas juba kutsutakse nimega PHP2SHELL, ei saanud kohalikud IT-juhid oodata. CERT-EU ja kohalikud eksperdid soovivad süsteemid, mida kohe hetkel uuendada ei saa, ajutiselt avalikust internetist lahti ühendada.

Kaitsemeetmetega liitus ka Cloudflare, mis lülitas oma veebirakenduste tulemüürile (WAF) sisse esmased reeglid rünnakute tõrjumiseks. Siiski rõhutas Cloudflare'i tehnoloogiajuht Dane Knecht, et tegemist on vaid ajutise plaastriga lahtisel haaval ning päris lahenduse toob ainult ametlik süsteemiuuendus.

Samal seisukohal on PHP tuumikarendaja Gina Peter Banyard, kes hoiatas otsekoheselt, et imevitsa ei ole ja serveri seadistuste näppimine (nagu failiüleslaadimise progressi väljalülitamine) ei taga kaitset: ainus reaalne rohi on

paigaldada ametlik turvavärskendus.



Mida peavad veebihaldurid kohe tegema?

Kui haldad ise veebiserverit või virtuaalmasinat, ei tasu loota pelgalt heale õnnele. Arvesse tuleb võtta, et ametlikud turvapaigad tehakse kättesaadavaks üksnes toetatud versioonidele (PHP 8.2 ja uuemad). Vanemad versioonid – sealhulgas laialt levinud PHP 7 ja PHP 8.1, aga ametlikku tuge ei saa, mistõttu tuleb need võimalikult kiiresti ajakohasele versioonile üle viia.

Administraatoritel tasub kohe astuda järgmised sammud:

- Uuendada PHP paigatud versioonile esimesel võimalusel.
- Kontrollida tagantjärele serverite logisid (eriti alates 2026. aasta suvest), otsides kahtlasi veebikoode (*web shell*), tundmatuid faile, volitamata administraatorikontosid ja anomaalseid väljuvaid võrguühendusi.
- Kui kohene uuendamine pole võimalik, piirata ajutiselt ligipääsu haldusliidestele ja avalikele vormidele.

[Uuenda nüüd!](#)

- [Uudised](#)
- [Serverid](#)
- [Turvalisus](#)

Pilt

