Signal Vulnerability Lets Malicious Callers Block Hang-Ups

Affecting the open source calling library RingRTC, the bug prevented calls from ending properly.

The post Signal Vulnerability Lets Malicious Callers Block Hang-Ups appeared first on SecurityWeek.

https://www.securityweek.com/signal-vulnerability-lets-malicious-callers-block-hang-ups/

Tech and Security Companies Respond to PHP2Shell Vulnerabilities

Vendors are checking their products for PHP2Shell, security firms are shipping detections, and governments are urging immediate patching.

The post Tech and Security Companies Respond to PHP2Shell Vulnerabilities appeared first on SecurityWeek.

https://www.securityweek.com/tech-and-security-companies-respond-to-php2shell-vulnerabilities/

Advertisers Pull Meta Ads That Had Unwanted AI Glow-ups

Under Meta’s new terms coming into play Oct 30, advertisers are “solely responsible” for whatever its AI creates https://www.adweek.com/media/advertisers-pull-meta-ads-that-had-unwanted-ai-glow-ups/

PHP, falla scoperta da OpenAI mette a rischio fino al 70% dei siti web in tutto il mondo

Una grave vulnerabilità nel codice di **PHP**, uno dei linguaggi di programmazione più utilizzati sul web, sta provocando un’allerta internazionale e una corsa agli aggiornamenti di sicurezza.

La falla è stata individuata inizialmente ad agosto dai ricercatori della startup di cybersecurity **Calif.io** utilizzando **GPT-5.6 Sol**, il modello di **OpenAI.** La scoperta è stata comunicata agli sviluppatori di PHP, che hanno successivamente creato un gruppo di lavoro insieme a **Calif.io, OpenAI, Google** e altri soggetti per sviluppare una soluzione.

Secondo The Information, durante le verifiche gli esperti di **Wiz**, la divisione di sicurezza informatica di **Google**, hanno individuato anche altre vulnerabilità collegate.

Il risultato è una serie di falle considerate particolarmente

gravi perché potrebbero consentire, in determinate configurazioni, attacchi di Remote Code Execution: un aggressore potrebbe cioè eseguire codice a distanza sul server compromesso, con la possibilità di installare malware, accedere ai database o intervenire sui file del sistema.

Fino al 70% dei siti web potenzialmente interessato

Secondo i ricercatori di Wiz citati da The Information, le vulnerabilità potrebbero mettere a rischio fino al 70% dei siti web mondiali se gli aggiornamenti non venissero applicati rapidamente. Gli esperti le hanno definite “le vulnerabilità più gravi mai scoperte dall’AI, se non tra le più gravi nella storia del software”.

PHP è infatti alla base di una parte enorme del web e viene utilizzato direttamente o indirettamente da piattaforme come **WordPress, Drupal, Joomla e Magento**, oltre che da servizi di hosting, pannelli di controllo e numerosi software. Secondo le informazioni disponibili, il codice vulnerabile sarebbe rimasto inosservato per molti anni. The Information riferisce che i ricercatori parlano addirittura di una falla presente da decenni, mentre altre ricostruzioni indicano un periodo superiore ai dieci anni.

L’AI ha trovato ciò che gli esperti non avevano visto

Calif.io avrebbe individuato la vulnerabilità utilizzando GPT-5.6 Sol nell’ambito di attività di ricerca sulla sicurezza. La scoperta rientra nel programma Patch the Planet, che coinvolge ricercatori e aziende impegnati nell’utilizzo dei modelli AI avanzati per individuare vulnerabilità nel software.

Il caso mostra come i modelli di frontiera stiano diventando strumenti sempre più potenti anche nella ricerca di bug complessi.

Secondo The Information, la vulnerabilità PHP rappresenta uno degli esempi più evidenti di quanto i modelli AI abbiano ormai raggiunto capacità estremamente avanzate nell'analisi del codice, arrivando a individuare problemi rimasti invisibili per anni durante revisioni e controlli condotti dagli sviluppatori.

La stessa capacità, tuttavia, pone un problema evidente: gli strumenti che possono essere utilizzati per individuare una vulnerabilità e correggerla possono anche rendere più semplice la ricerca di falle da sfruttare negli attacchi.

La fuga di informazioni accelera la corsa alla patch

Gli sviluppatori di PHP avevano inizialmente previsto di rendere pubblici i dettagli della vulnerabilità insieme a una soluzione completa. La situazione sarebbe però precipitata dopo la diffusione sui social media di informazioni sulla falla, aumentando il rischio che gruppi criminali potessero sviluppare rapidamente strumenti di attacco.

La PHP Foundation e gli sviluppatori hanno quindi invitato i gestori dei siti ad applicare il nuovo aggiornamento di sicurezza il prima possibile.

La **National Security Agency** statunitense ha invitato aziende e amministrazioni pubbliche ad aggiornare rapidamente i sistemi, arrivando a indicare come possibile misura precauzionale la temporanea disattivazione dei siti pubblicamente accessibili quando non sia possibile applicare immediatamente la patch. Avvisi simili sono arrivati dalle autorità di cybersecurity del Regno Unito, dell'Unione europea, del Giappone e

dell’Australia.

Siti pubblici temporaneamente offline

In Finlandia alcuni servizi web governativi sono stati temporaneamente disattivati come misura precauzionale, mentre nei Paesi Bassi anche siti istituzionali sono stati messi offline in attesa degli aggiornamenti.

In Germania il rischio è stato classificato a un livello particolarmente elevato e alcune strutture, compresi ospedali, avrebbero temporaneamente disattivato servizi online considerati potenzialmente esposti. Anche in Francia diversi siti delle prefetture sono stati resi temporaneamente inaccessibili per attività definite di “manutenzione preventiva”.

La scelta di spegnere temporaneamente un servizio non significa necessariamente che il sistema sia stato compromesso: in molti casi si tratta di una misura precauzionale per eliminare la finestra temporale durante la quale un attaccante potrebbe sfruttare la vulnerabilità prima dell’installazione della patch.

Primi tentativi di attacco già rilevati

Dane Knecht, responsabile tecnologico di Cloudflare, ha riferito che l’azienda sta già osservando i primi tentativi di sfruttamento delle vulnerabilità. *“Stiamo osservando attacchi iniziali emergenti e stiamo aggiornando le mitigazioni man mano che appaiono nuovi vettori”,* ha spiegato.

La priorità per aziende, pubbliche amministrazioni e gestori di siti è quindi verificare rapidamente la versione di PHP

utilizzata e installare gli aggiornamenti messi a disposizione dagli sviluppatori.

Il rischio per WordPress

Particolare attenzione riguarda **WordPress**, il sistema di gestione dei contenuti utilizzato da una quota molto elevata dei siti web mondiali. La vulnerabilità non implica che ogni sito WordPress possa essere automaticamente compromesso. Il rischio dipende dalla versione di PHP, dalla configurazione del server e dal modo in cui il linguaggio viene utilizzato.

La diffusione di WordPress rende però il problema particolarmente delicato: molti siti vengono gestiti attraverso hosting condivisi o infrastrutture nelle quali gli aggiornamenti di PHP dipendono dal provider e non direttamente dal proprietario del sito. Lo stesso vale per piattaforme costruite con Drupal, Joomla, Magento e altri sistemi basati sul linguaggio.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/php-falla-scoperta-da-openai-mette-a-rischio-fino-al-70-dei-siti-web-in-tutto-il-mondo/591670/

Splunk, SolarWinds Release Fresh Security Updates

Patched vulnerabilities could allow attackers to execute code, elevate privileges, and leak sensitive information.

The post Splunk, SolarWinds Release Fresh Security Updates appeared first on SecurityWeek.

https://www.securityweek.com/splunk-solarwinds-release-fresh-security-updates/

Week of Oct. 5 Morning News Ratings: CBS Mornings Grows

Today also registered gains in the advertiser-coveted demo https://www.adweek.com/tvnewser/week-of-oct-5-2026-morning-news-ratings/

2026 FIFA World Cup Provided a Big Kick to NBCU Ad Sales

Telemundo and Peacock benefited from Spanish-language World Cup rights with $224 million in ad revenue in Q3. https://www.adweek.com/convergent-tv/2026-fifa-world-cup-provided-a-big-kick-to-nbcu-ad-sales/

Cisco Patches 34 Vulnerabilities Across Multiple Products

Critical-severity security defects could lead to command execution, authentication bypass, and XSS attacks.

The post Cisco Patches 34 Vulnerabilities Across Multiple Products appeared first on SecurityWeek.

https://www.securityweek.com/cisco-patches-34-vulnerabilities-across-multiple-products/

Shannon Nunn Rounds Out LePub NY Leadership Team as CEO

Former president of Special US will lead the global creative network's new stateside hub. https://www.adweek.com/agencies/shannon-nunn-rounds-out-lepub-ny-leadership-team-as-ceo/

PHP2Shell Exploitation Started Days Before Patches

Initial attempts were observed on October 17, and mass activity began shortly after patches were released.

The post PHP2Shell Exploitation Started Days Before Patches appeared first on SecurityWeek.

https://www.securityweek.com/php2shell-exploitation-started-days-before-patches/