PHP2Shell: दो गंभीर भेद्यताएँ, और इंटरनेट की अदृश्य नींव का संकट

विज्ञान और प्रौद्योगिकी (साइबर-सुरक्षा) | समाचार संदर्भ: 20-21 अक्टूबर 2026 (घोषणा और सुधार); CERT-EU परामर्श 21 अक्टूबर 2026 | प्रकाशित: 23 अक्टूबर 2026

खबरों में क्यों

20 अक्टूबर 2026 को PHP परियोजना ने दो गंभीर सुरक्षा-भेद्यताओं की घोषणा की और 21 अक्टूबर 2026 को (13:30 UTC) PHP संस्करण 8.5.12, 8.4.27, 8.3.36 और 8.2.35 में सुधार जारी किए (CERT-EU परामर्श, 21 अक्टूबर 2026)। सावधानी के तौर पर कई सेवाएँ अस्थायी रूप से ऑफ़लाइन हुईं — जापान के वित्त मंत्रालय और स्वास्थ्य मंत्रालय की साइटों के कुछ भाग (जापान टाइम्स, 22 अक्टूबर 2026), विकिपीडिया की कई सेवाएँ (विकिमीडिया), रॉटरडैम बंदरगाह, नीदरलैंड के कई अस्पताल तथा नीदरलैंड, फ़िनलैंड और डेनमार्क की कुछ सरकारी साइटें (ProjectDiscovery, 21 अक्टूबर 2026), और अमेरिकी HR मंच BambooHR (php2shell.uk टाइमलाइन)। CERT-In ने 21 अक्टूबर 2026 को गंभीर-स्तरीय परामर्श जारी किया (इंडियन एक्सप्रेस रिपोर्ट, 22 अक्टूबर 2026; cert-in.org.in का प्रत्यक्ष पृष्ठ नहीं खुल सका); अमेरिका की CISA/NSA और ब्रिटेन का NCSC भी चेतावनी जारी कर चुके थे।

भेद्यताएँ क्या हैं? (दोनों CVSS 9.2)

- **CVE-2026-109618 (OOM भ्रष्टाचार):** मेमोरी-सीमा पार होने पर PHP अनुरोध को बीच में रोक देता है; आंशिक रूप से बना आंतरिक डेटा सफ़ाई के दौरान “मान्य” समझा जा सकता है — परिणाम: मेमोरी भ्रष्टाचार और दूरस्थ कोड-निष्पादन (RCE)।
- **CVE-2026-109619 (पुरानी वैश्विक स्थिति):** एक अनुरोध की मुक्त हो चुकी मेमोरी के संदर्भ बचे रह सकते हैं; उसी वर्कर का अगला अनुरोध इस अवशिष्ट स्थिति का उपयोग कर सकता है — RCE संभव।
- दोनों में आक्रमणकर्ता को खाते या भौतिक पहुँच की ज़रूरत नहीं; PHP 7.4, 8.0 और 8.1 के लिए न्यूनतम स्रोत-बैकपोर्ट भी प्रकाशित हुए।

PHP क्यों इतना महत्वपूर्ण?

PHP मुक्त-स्रोत, स्वयंसेवक-रखरखाव वाली भाषा है जो पहचान योग्य सर्वर-साइड भाषा वाली लगभग 70% वेबसाइटों को चलाती है; वर्डप्रेस (विश्व की 40% से अधिक वेबसाइटें) PHP पर ही बना है। छोटी साइटें साझा होस्टिंग पर होती हैं, जहाँ मालिक सर्वर नियंत्रित नहीं करता; PHP कंटेंट-प्रबंधन प्रणालियों और तृतीय-पक्ष उत्पादों में अदृश्य रूप से धँसा रहता है — इसलिए चुनौती सिर्फ पैच लगाना नहीं, हर PHP इंस्टेंस का पता लगाना है। CERT-EU ने सलाह दी कि जो तुरंत पैच न कर सकें, वे असुरक्षित सिस्टम ऑफ़लाइन रखें।

विश्लेषण

यह प्रकरण दिखाता है कि इंटरनेट की बुनियादी संरचना दशकों पुराने, स्वयंसेवक-रखरखाव वाले कोड पर टिकी है। AI उपकरणों ने खोज-शोध में मदद की, पर वही तकनीक आक्रमणकर्ता की भी गति बढ़ा सकती है — प्रतिक्रिया-खिड़की सिकुड़ती है। साइबर-लचक का अर्थ अब पैच की गति जितना ही छिपी निर्भरताओं की दृश्यता भी है।

खोज का श्रेय-विवरण (PHP फ़ाउंडेशन के अनुसार)

PHP फ़ाउंडेशन ने PHP परियोजना को "Patch the Planet" (सुरक्षा-शोध कार्यक्रम, जिसमें स्वतंत्र सुरक्षा-फ़र्में सॉफ़्टवेयर की ऑडिट — व्यवस्थित सुरक्षा-जाँच — करती हैं) में शामिल कराया था। इसी के तहत सुरक्षा-फ़र्म Calif ने 30 जुलाई 2026 को PHP की ऑडिट शुरू की; 11 अगस्त 2026 को Calif के शोधकर्ता Ryan A ने उसी मूल-कारण (root cause — किसी दोष का वह मूल तकनीकी कारण जिससे सभी आक्रमण-मार्ग बनते हैं) वाली बिना-शर्त RCE रिपोर्ट की। Wiz ने 24 अगस्त को अपनी रिपोर्ट दी; OpenAI ने स्वतंत्र रूप से वही मूल-कारण रिपोर्ट किया और 18 सितंबर को आगे के आक्रमण-मार्ग बताए; Trail of Bits भी PHP की ऑडिट कर रही थी। आधिकारिक सलाहकार-दस्तावेज़ रिपोर्टर्स को lcfr-hax, sagitzadik-wiz, tomash-areion और amyb-oai के नाम से श्रेय देते हैं।

परीक्षा की दृष्टि से

- **प्रारंभिक:** CVE और CVSS क्या हैं; RCE (दूरस्थ कोड-निष्पादन); CERT-In, CERT-EU, CISA, ENISA जैसी एजेंसियों की भूमिका; PHP और वर्डप्रेस का विस्तार।
- **मुख्य परीक्षा (GS-3):** साइबर-सुरक्षा; मुक्त-स्रोत सॉफ़्टवेयर पर निर्भरता और आपूर्ति-शृंखला जोखिम; critical information infrastructure की सुरक्षा।

मुख्य परीक्षा अभ्यास प्रश्न

"PHP जैसे व्यापक रूप से प्रयुक्त ओपन-सोर्स प्लेटफ़ॉर्म में गंभीर भेद्यताएँ कई देशों की सरकारी और वित्तीय सेवाओं को एक साथ प्रभावित कर सकती हैं। सॉफ्टवेयर आपूर्ति-शृंखला की इस निर्भरता के जोखिमों और शमन उपायों की चर्चा कीजिए।"
(250 शब्द)

उत्तर की रूपरेखा:

भूमिका में: संदर्भ रखें: 20 अक्टूबर 2026 को PHP परियोजना ने दो गंभीर भेद्यताओं (दोनों CVSS 9.2, दूरस्थ कोड-निष्पादन संभव) की घोषणा की और 21 अक्टूबर 2026 को सुधार जारी किए (CERT-EU परामर्श)। कई देशों की कुछ सरकारी और अन्य सेवाएँ सावधानी के तौर पर अस्थायी रूप से ऑफ़लाइन हुईं; यह विवरण लेख में सूचीबद्ध स्रोतों के अनुसार ही रखें।

मुख्य भाग में: पहले खंड में निर्भरता के जोखिम रखें: PHP मुक्त-स्रोत, स्वयंसेवक-रखरखाव वाली भाषा है और लगभग 70% पहचान योग्य सर्वर-साइड वेबसाइटों को चलाती है, वर्डप्रेस उसी पर बना है (ये व्यापक रूप से उद्धृत अनुमान हैं); साझा होस्टिंग में मालिक का सर्वर पर नियंत्रण नहीं रहता; PHP कंटेंट-प्रबंधन प्रणालियों और तृतीय-पक्ष उत्पादों में छिपा रहता है, इसलिए चुनौती केवल पैच लगाना नहीं, हर PHP इंस्टेंस का पता लगाना है; और AI उपकरण खोज में मदद करने के साथ आक्रमणकर्ता की गति भी बढ़ा सकते हैं। दूसरे खंड में शमन उपाय रखें: सुधारित संस्करणों में तुरंत पैच, जो पैच न कर सकें उनके लिए असुरक्षित सिस्टम ऑफ़लाइन रखना (CERT-EU की सलाह), छिपी निर्भरताओं की दृश्यता, तथा CERT-In जैसी एजेंसियों के परामर्श और अंतर्राष्ट्रीय समन्वय की भूमिका; CERT-In परामर्श का मूल पृष्ठ नहीं खुला था, इसलिए उसका विवरण समाचार-रिपोर्ट पर आधारित बताएँ। लेख में न दिए गए आँकड़े, घटनाएँ या नीतियाँ न जोड़ें।

निष्कर्ष में: निष्कर्ष में कहें कि साइबर-लचक का अर्थ पैच की गति के साथ छिपी निर्भरताओं की दृश्यता भी है, और मुक्त-स्रोत आधारित बुनियादी ढाँचे की सुरक्षा साझा ज़िम्मेदारी है। ऑफ़लाइन हुई सेवाओं के संगठन-स्तरीय विवरण स्वतंत्र रूप से सत्यापित नहीं हैं, यह सीमा रखें।

स्रोत और सीमाएँ

- CERT-EU सुरक्षा परामर्श 2026-018, 21 अक्टूबर 2026 (पढ़ा; CVE-संख्या, CVSS 9.2, संस्करण 8.5.12/8.4.27/8.3.36/8.2.35, 13:30 UTC सत्यापित): https://www.cert.europa.eu/publications/security-advisories/2026-018/
- PHP Foundation, 21 अक्टूबर 2026 (पढ़ा): https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/
- ENISA संयुक्त बयान (पढ़ा): https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities
- NCSC (ब्रिटेन) (पढ़ा): https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php
- Project Discovery तकनीकी विश्लेषण (पढ़ा; Wiz की तकनीकी रिसर्च का संदर्भ): https://projectdiscovery.io/research/php2shell
- Indian Express, 22 अक्टूबर 2026 (पढ़ा; CERT-In गंभीर-स्तरीय परामर्श 21 अक्टूबर, NSA चेतावनी, CVSS 9.2, सुधारित संस्करण): https://indianexpress.com/article/technology/cert-in-php-vulnerability-alert-india-cybersecurity-warning-us-nsa-php-alert-10931962/
- Japan Times (Reuters), 22 अक्टूबर 2026 (पढ़ा; जापान के वित्त/स्वास्थ्य मंत्रालय की साइटें आंशिक ऑफ़लाइन): https://www.japantimes.co.jp/business/2026/10/22/tech/japan-php-vulnerabilities/
- ProjectDiscovery रिसर्च, 21 अक्टूबर 2026 (पढ़ा; विकिमीडिया/रॉटरडैम/अस्पताल/यूरोपीय सरकारी साइटें ऑफ़लाइन; CISA, NSA, NCSC, CERT-EU चेतावनियाँ): https://projectdiscovery.io/research/php2shell
- php2shell.uk डिस्क्लोज़र टाइमलाइन (पढ़ा; BambooHR 21 अक्टूबर 11:51 UTC ऑफ़लाइन): https://php2shell.uk/timeline
- **सीमाएँ:** CERT-In परामर्श का मूल पृष्ठ (cert-in.org.in) तकनीकी रोक के कारण प्रत्यक्ष नहीं खोला जा सका; विवरण IE रिपोर्ट पर आधारित है। ऑफ़लाइन सेवाओं का विवरण ऊपर सूचीबद्ध स्रोतों से है; संबंधित संगठनों के अपने स्टेटस-पृष्ठ अलग से नहीं खोले गए। “70%”/”40%” आँकड़े व्यापक रूप से उद्धृत अनुमान हैं।

अक्सर पूछे जाने वाले प्रश्न (FAQ)

संक्षिप्त उत्तर: 20 अक्टूबर 2026 को PHP परियोजना ने दो गंभीर सुरक्षा-भेद्यताओं की घोषणा की और 21 अक्टूबर 2026 को (13:30 UTC) PHP संस्करण 8.5.12, 8.4.27, 8.3.36 और 8.2.35 में सुधार जारी किए (CERT-EU परामर्श, 21 अक्टूबर 2026)। सावधानी के तौर पर कई सेवाएँ अस्थायी रूप से ऑफ़लाइन हुईं - जापान के वित्त मंत्रालय और स्वास्थ्य मंत्रालय की साइटों के कुछ भाग (जापान टाइम्स, 22 अक्टूबर 2026), विकिपीडिया की कई सेवाएँ (विकिमीडिया), रॉटरडैम बंदरगाह, नीदरलैंड के कई अस्पताल तथा नीदरलैंड, फ़िनलैंड और डेनमार्क की कुछ सरकारी साइटें (ProjectDiscovery, 21 अक्टूबर 2026), और अमेरिकी HR मंच BambooHR (php2shell.uk टाइमलाइन)।

प्रश्न: PHP2Shell संबंधी सुधार कब और किन PHP संस्करणों में जारी हुए?

20 अक्टूबर 2026 को PHP परियोजना ने दो गंभीर सुरक्षा-भेद्यताओं की घोषणा की और 21 अक्टूबर 2026 को (13:30 UTC) PHP संस्करण 8.5.12, 8.4.27, 8.3.36 और 8.2.35 में सुधार जारी किए (CERT-EU परामर्श, 21 अक्टूबर 2026)। सावधानी के तौर पर कई सेवाएँ अस्थायी रूप से ऑफ़लाइन हुईं - जापान के वित्त मंत्रालय और स्वास्थ्य मंत्रालय की साइटों के कुछ भाग (जापान टाइम्स, 22 अक्टूबर 2026), विकिपीडिया की कई सेवाएँ (विकिमीडिया), रॉटरडैम बंदरगाह, नीदरलैंड के कई अस्पताल तथा

नीदरलैंड, फ़िनलैंड और डेनमार्क की कुछ सरकारी साइटें (ProjectDiscovery, 21 अक्टूबर 2026), और अमेरिकी HR मंच BambooHR (php2shell.uk टाइमलाइन)। CERT-In ने 21 अक्टूबर 2026 को गंभीर-स्तरीय परामर्श जारी किया (इंडियन एक्सप्रेस रिपोर्ट, 22 अक्टूबर 2026; cert-in.org.in का प्रत्यक्ष पृष्ठ नहीं खुल सका); अमेरिका की CISA/NSA और ब्रिटेन का NCSC भी चेतावनी जारी कर चुके थे।

प्रश्न: PHP सुरक्षा में छिपी निर्भरताओं का पता लगाना क्यों जरूरी है?

PHP मुक्त-स्रोत, स्वयंसेवक-रखरखाव वाली भाषा है जो पहचान योग्य सर्वर-साइड भाषा वाली लगभग 70% वेबसाइटों को चलाती है; वर्डप्रेस (विश्व की 40% से अधिक वेबसाइटें) PHP पर ही बना है। छोटी साइटें साझा होस्टिंग पर होती हैं, जहाँ मालिक सर्वर नियंत्रित नहीं करता; PHP कंटेंट-प्रबंधन प्रणालियों और तृतीय-पक्ष उत्पादों में अदृश्य रूप से धँसा रहता है - इसलिए चुनौती सिर्फ पैच लगाना नहीं, हर PHP इंस्टेंस का पता लगाना है। CERT-EU ने सलाह दी कि जो तुरंत पैच न कर सकें, वे असुरक्षित सिस्टम ऑफ़लाइन रखें।

प्रश्न: PHP2Shell प्रकरण साइबर-लचक के बारे में क्या दिखाता है?

यह प्रकरण दिखाता है कि इंटरनेट की बुनियादी संरचना दशकों पुराने, स्वयंसेवक-रखरखाव वाले कोड पर टिकी है। AI उपकरणों ने खोज-शोध में मदद की, पर वही तकनीक आक्रमणकर्ता की भी गति बढ़ा सकती है - प्रतिक्रिया-खिड़की सिकुड़ती है। साइबर-लचक का अर्थ अब पैच की गति जितना ही छिपी निर्भरताओं की दृश्यता भी है।