प्रोजेक्ट ग्लासविंग और AI साइबर सुरक्षा — प्रमुख तथ्य

विज्ञान और प्रौद्योगिकी (प्रारंभिक परीक्षा: सामान्य अध्ययन) | समाचार संदर्भ: जून 2026 | प्रकाशित: 24 अक्टूबर 2026

खबरों में क्यों

जून 2026 की शुरुआत में एक प्रमुख AI कंपनी ने अपनी साइबर सुरक्षा पहल 'प्रोजेक्ट ग्लासविंग' का विस्तार करने की बात कही। पहले चरण में करीब 50 चुनिंदा संगठन इससे जुड़े थे। नई घोषणा के अनुसार लगभग 150 और संगठन जोड़े जाने थे, यानी कुल संख्या करीब 200 के पास पहुंचती। साथ ही शर्त रखी गई कि पहुंच देने से पहले हर संगठन की सुरक्षा-संबंधी जांच होगी। इसलिए सूची में शामिल होने को तुरंत पहुंच मिल जाने का प्रमाण नहीं माना जा सकता।

इसी दौरान ऐसी रिपोर्ट भी आईं कि भारत की कुछ सरकारी साइबर एजेंसियों को इस पहल की पहुंच मिल रही है और देश की बड़ी सूचना-प्रौद्योगिकी कंपनियों से संपर्क चल रहा है। ये जानकारियां अधिकारियों के हवाले से थीं; किसी भी नाम की स्वतंत्र, सार्वजनिक आधिकारिक पुष्टि यहां प्रस्तुत नहीं की जा रही।

साल के बाद के महीनों में यह पहल एक ही रूप में नहीं रही। 6 अक्टूबर 2026 को ग्लासविंग को कंपनी के साइबर सत्यापन कार्यक्रम के साथ मिलाकर एक बड़ी व्यवस्था बनाई गई। 8 अक्टूबर को खुले स्रोत (ओपन-सोर्स) सॉफ्टवेयर की जांच के लिए एक स्वैच्छिक स्कैनर सेवा शुरू हुई। इसलिए जून की शुरुआती सीमित साझेदारी को ही इस पहल का अंतिम और स्थिर रूप नहीं समझना चाहिए।

पहले समझें: सुरक्षा भेद्यता क्या है?

किसी सॉफ्टवेयर या उसकी सेटिंग में मौजूद ऐसी खामी, जिसका गलत इस्तेमाल करके अनधिकृत काम किया जा सके, सुरक्षा भेद्यता (वल्नरेबिलिटी) कहलाती है। हर तकनीकी गड़बड़ी उतनी ही खतरनाक नहीं होती। खतरे का आकलन करने के लिए यह देखना होता है कि उस खामी का वास्तव में दुरुपयोग संभव है या नहीं, उससे कितना नुकसान हो सकता है और कौन-कौन से संस्करण प्रभावित हैं।

ग्लासविंग क्या है?

यह पहल चुनिंदा संगठनों को एक उन्नत AI सेवा की मदद से अपने महत्वपूर्ण सॉफ्टवेयर में सुरक्षा कमजोरियां खोजने और उन्हें दूर करने का अवसर देती थी। कंपनी के अनुसार इसमें इस्तेमाल होने वाला AI मॉडल जटिल कोड की जांच कर ऐसी कमजोरियों की ओर ध्यान दिला सकता है, जिन्हें खोजना अन्यथा कठिन होता है।

ध्यान रहे कि यह आम उपयोगकर्ता के लिए खुली कोई सेवा या किसी तरह की सार्वभौमिक सुरक्षा-गारंटी नहीं थी। पहुंच सीमित और शर्तों के साथ थी, और उद्देश्य रक्षात्मक (डिफेंसिव) उपयोग था।

मुख्य तथ्य

- **प्रोजेक्ट ग्लासविंग:** AI का साइबर सुरक्षा में प्रयोग करने वाली पहल; कमजोरियों (वल्नरेबिलिटी) की खोज में AI की भूमिका पर केंद्रित।
- **वल्नरेबिलिटी:** सॉफ्टवेयर की वह खामी जिसका दुरुपयोग हमलावर कर सकता है।
- **दोहरी उपयोगिता (ड्युअल-यूज़):** वही AI क्षमता सुरक्षा-सुधार और हमले दोनों में काम आ सकती है — यही नीति-प्रश्न है।
- **खोज से सुधार तक की दूरी:** कमजोरी मिलना और पैच/सुधार लागू होना अलग चरण; खोज की सफलता को पूर्ण सुरक्षा का प्रमाण नहीं मानना चाहिए।
- **जिम्मेदार सूचना (रिस्पॉन्सिबल डिस्क्लोजर):** कमजोरी को पहले निर्माता/संस्था को सूचित कर सुधार का अवसर देना, फिर प्रकाशन।
- **भारत के लिए महत्व:** डिजिटल सेवाओं (भुगतान, पहचान, सरकारी पोर्टल) की सुरक्षा में AI-आधारित खोज और जिम्मेदार सूचना दोनों प्रासंगिक।

परीक्षा की दृष्टि से

प्रारंभिक परीक्षा के लिए याद रखने योग्य: ग्लासविंग का उद्देश्य, वल्नरेबिलिटी की परिभाषा, AI की दोहरी उपयोगिता, खोज बनाम सुधार का भेद, जिम्मेदार सूचना की प्रक्रिया। नीति-विश्लेषण और भारत-प्रभाव का विस्तृत मूल्यांकन मुख्य परीक्षा लेख में (लिंक नीचे स्रोत में)।

प्रारंभिक परीक्षा अभ्यास:

प्रश्न 1. साइबर सुरक्षा के संबंध में निम्नलिखित कथनों पर विचार कीजिए:

1. AI से मिली संभावित सुरक्षा कमजोरी को तकनीकी सत्यापन की जरूरत हो सकती है।
2. किसी सुधार का उपलब्ध हो जाना सभी प्रभावित प्रणालियों में उसके लागू होने का प्रमाण है।
3. जिम्मेदार भेद्यता खुलासा संबंधित पक्षों के बीच जांच और सुधार का समन्वय कर सकता है।

उपर्युक्त में से कौन-से कथन सही हैं?

(a) केवल 1 और 2

(b) केवल 1 और 3

(c) केवल 2 और 3

(d) 1, 2 और 3

उत्तर और कारण देखें
उत्तर: (b)।
संभावित रिपोर्ट गलत या दोहराई हुई हो सकती है। सुधार जारी होना और उसका हर प्रभावित सिस्टम पर लागू होना अलग चरण हैं। जिम्मेदार खुलासा जांच तथा सुधार में समन्वय करता है।

स्रोत और सीमाएँ

- 2 जून 2026: ग्लासविंग विस्तार की कंपनी घोषणा
- ग्लासविंग विस्तार और दावों पर स्वतंत्र रिपोर्ट
- जून 2026: भारतीय संस्थाओं की पहुंच पर रिपोर्ट
- CERT-In: जिम्मेदार भेद्यता खुलासा और समन्वय नीति
- NCIIPC की आधिकारिक भूमिका
- 6 अक्टूबर 2026: साइबर सत्यापन कार्यक्रम में बदलाव
- 8 अक्टूबर 2026: स्वैच्छिक OSS Scanner और उसकी सीमाएं
- **सीमाएँ:** जून का विस्तार और अक्टूबर के बाद के बदलाव (6 अक्टूबर CVP एकीकरण, 8 अक्टूबर OSS स्कैनर) अलग चरण के रूप में बताए गए हैं। किसी खोज को सत्यापित समस्या, जांचा गया पैच या तैनात सुधार नहीं माना गया। कंपनी के प्रदर्शन-आँकड़े और पूर्वानुमान नहीं दिए गए। भारत में पहुंच के बारे में बिना नाम अधिकारी के हवाले रिपोर्टिंग है; किसी एजेंसी की पुष्टि का दावा नहीं। CERT-In/NCIIPC को प्राथमिक संदर्भ के रूप में बताया गया है; रिपोर्टिंग परीक्षण की अनुमति नहीं बनाती। कोई शोषण-निर्देश या सार्वभौमिक AI-सुरक्षा दावा नहीं।

इसी विषय का मुख्य परीक्षा (विश्लेषण) लेख: प्रोजेक्ट ग्लासविंग: AI से साइबर सुरक्षा में खोज से सुधार तक की दूरी