समाचार वाणी
ख़बर जो करें असर !

नाशिक | Thursday, 24 September 2026

3.5 अरब WhatsApp यूजर्स का डेटा लीक ! मेटा की लापरवाही से उजागर हुआ अब तक का सबसे बड़ा नंबर लीक

Publisher

Published on 19 Nov 2025

WhatsApp की सुरक्षा को लेकर दुनिया भर में जिस भरोसे की बात की जाती है, वह एक बार फिर सवालों के घेरे में है। दावा किया जा रहा है कि मैसेजिंग प्लेटफॉर्म के करीब 3.5 अरब यूजर्स के मोबाइल नंबर लीक हो गए हैं। यह संख्या दुनिया भर के कुल WhatsApp यूजर्स का लगभग पूरा हिस्सा मानी जा रही है। हैरान करने वाली बात यह है कि इस लीक के पीछे किसी हैकिंग गैंग या साइबर क्रिमिनल का हाथ नहीं, बल्कि व्हाट्सऐप की पैरेंट कंपनी मेटा की लापरवाही को जिम्मेदार ठहराया जा रहा है। रिपोर्ट्स में कहा गया है कि कंपनी को इस खामी की जानकारी आठ साल पहले से थी, लेकिन उसने इसे नजरअंदाज कर दिया। अब इस खुलासे को इतिहास के सबसे बड़े डेटा लीक के तौर पर देखा जा रहा है।

ऑस्ट्रिया की यूनिवर्सिटी ऑफ वियना के कुछ साइबर रिसर्चर्स ने इस चौंकाने वाले मामले का खुलासा किया है। वायर्ड की एक रिपोर्ट में बताया गया है कि रिसर्चर्स ने WhatsApp में एक बेहद साधारण लेकिन बेहद खतरनाक सुरक्षा खामी को पकड़ लिया। उन्होंने पाया कि बिना किसी हैकिंग टूल या तकनीकी विशेषज्ञता के, कोई भी व्यक्ति WhatsApp पर दुनिया भर के 3.5 अरब फोन नंबरों की जानकारी निकाल सकता है। रिसर्चर्स ने केवल WhatsApp Web का इस्तेमाल किया और अरबों मोबाइल नंबर एक साथ सिस्टम में डालकर यह जांचने में कामयाबी हासिल की कि कौन-कौन सा नंबर WhatsApp पर रजिस्टर है।

यह सुरक्षा खामी बेहद सीधी थी—WhatsApp Web पर रजिस्टर किए गए नंबरों की वैधता की जांच करने की प्रक्रिया को ऑटोमेट कर दिया गया। इसके चलते लाखों नहीं, बल्कि अरबों फोन नंबरों को एक साथ स्कैन किया जा सका। रिसर्चर्स का कहना है कि यह डेटा किसी गलत व्यक्ति के हाथ लगता, तो वह इन नंबरों पर स्पैम, फ्रॉड कॉल्स, फिशिंग लिंक या अन्य धोखाधड़ी वाले संदेश भेज सकता था। यूजर्स की प्राइवेसी और सिक्योरिटी के लिहाज से यह स्थिति बेहद खतरनाक मानी जा रही है।

चौंकाने वाली बात यह है कि रिसर्चर्स का दावा है कि मेटा को इस सुरक्षा खामी की जानकारी कई साल पहले दी गई थी, लेकिन कंपनी ने इसे गंभीरता से नहीं लिया। हालांकि, अब जब मामला सामने आया है तो मेटा ने अपनी सफाई देते हुए कहा है कि यह

खामी मूल रूप से “डेटा लीक” की श्रेणी में नहीं आती, क्योंकि यूजर्स के फोन नंबर एक सार्वजनिक पहचानकर्ता के तौर पर कई जगह इस्तेमाल होते हैं। कंपनी के अनुसार इस प्रक्रिया से केवल यह पता चलता है कि संबंधित नंबर WhatsApp पर मौजूद है या नहीं। लेकिन विशेषज्ञ इसका विरोध करते हुए कह रहे हैं कि इतनी बड़ी संख्या में फोन नंबरों की पुष्टि करना खुद एक बड़ा खतरा है और इसका दुरुपयोग असंभव नहीं।

तकनीकी विशेषज्ञों का मानना है कि फोन नंबर जैसी निजी जानकारी किसी भी यूज़र की डिजिटल पहचान का मुख्य हिस्सा होती है। व्हाट्सऐप जैसी एन्क्रिप्शन आधारित ऐप में यदि नंबरों का ऐसा बड़े पैमाने पर एक्सपोज़र संभव है, तो यह यूजर्स के भरोसे को गहरा धक्का है। कई विशेषज्ञों ने इसे “एंड-टू-एंड एन्क्रिप्शन की सीमाओं का खुलासा” भी बताया है, क्योंकि एन्क्रिप्शन केवल चैट की सुरक्षा करता है, लेकिन पब्लिकली एक्सेसिबल नंबरों की सुरक्षा की जिम्मेदारी भी कंपनी की होती है।

रिपोर्ट्स का कहना है कि इस खामी से जुड़े डेटा सेट को कथित तौर पर डार्क वेब पर भी देखा गया है। हालांकि इसकी पुष्टि आधिकारिक तौर पर नहीं की गई है, लेकिन साइबर सुरक्षा विशेषज्ञों का कहना है कि इतनी बड़ी संख्या में नंबरों की उपलब्धता ऑनलाइन अपराधियों के लिए किसी सोने की खान से कम नहीं। इससे टेलीकॉल फ्रॉड, स्पैम कैंपेन और व्हाट्सऐप-आधारित फिशिंग अटैक की संख्या बढ़ने का खतरा है।

इस बीच, WhatsApp ने यह भी कहा है कि उन्होंने अपनी सिस्टम सिक्योरिटी में सुधार किए हैं और अब इस खामी को पहले की तरह एक्सप्लॉइट नहीं किया जा सकता। हालांकि, रिसर्चर्स का कहना है कि उन्हें अभी भी कई खामियां दिख रही हैं और ऐप को सुरक्षित बनाने के लिए बड़े स्तर पर सुधार की जरूरत है।

यूजर्स को सलाह दी जा रही है कि वे अपनी WhatsApp सेटिंग्स में जाकर प्राइवेसी सेटअप मजबूत करें, जैसे—प्रोफाइल फोटो, अबाउट और लास्ट सीन को केवल ‘My Contacts’ पर सेट करना। साथ ही अनजान नंबरों से आए लिंक न खोलने और किसी भी संदिग्ध गतिविधि पर तुरंत रिपोर्ट करने की भी सलाह दी जा रही है।

DISCLAIMER: the views/contents expressed/presented herein, within this advertorial and promotional feature are the sole and exclusive responsibility of individual clients/expert/their authorised representative/Publisher, to which effect, publication house/its representative/affiliates are not responsible/liable whatsover.