‘Log4Shell’ सुभेद्यता

प्रलिम्सि के लयि:

Log4Shell, ओपन-सोर्स लॉगगि सॉफ्टवेयर ‘Apache Log4J’, भेद्यता, एप्लीकेशन लॉगगि

मेन्स के लयि:

भारत और वशि्व पर ‘Log4Shell’ सुभेद्यता का प्रभाव।

चर्चा में क्यों

हाल ही में व्यापक रूप से उपयोग कयि जाने वाले ओपन-सोर्स लॉगगि सॉफ्टवेयर ‘Apache Log4J’ में ‘Log4Shell’ नामक एक गंभीर सुभेद्यता का पता चला है और इस सुभेद्यता का उपयोग साइबर हमलावरों द्वारा भारत सहति दुनयि भर के संगठनों के कंप्यूटरों को लक्षति करने के लयि कयि जा रहा है।

- सुभेद्यता एक ओपन-सोर्स लॉगगि लाइब्रेरी पर आधारति है, जसिका उपयोग उद्यमों और यहाँ तक कि सरकारी एजेंसयिों द्वारा प्रयोग कयि जाता है।

सुभेद्यता (Vulnerability)

- कंप्यूटर सुरक्षा में ‘सुभेद्यता’ का आशय कंप्यूटर सॉफ्टवेयर या हार्डवेयर में मौजूद कमज़ोरी से है, जसिका उपयोग एक कंप्यूटर सस्टिम के भीतर वशिेषाधकिार सीमाओं को पार करने (अर्थात् अनधकिृत कार्यों को करने) के लयि एक साइबर हमलावर द्वारा उपयोग कयि जासकता है।
- सुभेद्यता का उपयोग करने हेतु एक साइबर हमलावर के पास कम-से-कम एक ऐसा उपकरण या तकनीक होनी चाहयि, जो सस्टिम की कमज़ोरी से जुड़ सके और उसका लाभ उठा सके।

एप्लीकेशन लॉगगि

- एप्लीकेशन लॉगगि का आशय ‘एप्लीकेशन ईवेंट’ की एकत्रण की प्रक्रयिा से है। यह आईटी सस्टिम के भीतर अन्य इवेंट लॉग से भन्नि होता है जसिमें एक एप्लीकेशन इवेंट लॉग द्वारा एकत्र की गई जानकारी ऑपरेटगि सस्टिम के बजाय प्रत्येक व्यक्तगित एप्लीकेशन द्वारा नर्धिारति की जाती है।
- वे वभिन्नि बुनयिादी ढाँचे के घटकों में से प्रत्येक पर हमारे एप्लीकेशन कसि प्रकार चल रहे हैं, इसकी दृश्यता प्रदान करने में मदद करते हैं। लॉग डेटा में ‘मेमोरी एक्सेप्शन’ या हार्ड डस्कि त्रुटयिों जैसी जानकारी होती है।

प्रमुख बदिु

- **नाम**
  - इस सुभेद्यता को सामान्य तौर पर Log4Shell और आधकिारकि तौर पर ‘CVE-2021-44228’ नाम दयिा गया है।
  - ‘CVE’ नंबर दुनयिा भर में खोजी गई प्रत्येक सुभेद्यता को दी गई अद्वतिीय संख्या है।
  - इस सुभेद्यता का पता पहली बार उन वेबसाइटों पर लगाया गया था जो ‘माइनक्राफ्ट’ (Minecraft) नामक माइक्रोसॉफ्ट (Microsoft) के स्वामत्वि वाले गेम सर्वर को होस्ट कर रहे थे।

- **‘Log4j’ लाइब्रेरी:**
  - ‘Log4j’ गैर-लाभकारी अपाचे सॉफ्टवेयर फाउंडेशन के हस्सि के रूप में स्वयंसेवी प्रोग्रामर के एक समूह द्वारा बनाए रखा गया ओपन-सोर्स

सॉफ्टवेयर है और यह एक प्रमुख जावा-लॉगिंग फ्रेमवर्क है।
- 'Log4j' लाइब्रेरी प्रत्येक जावा-आधारित वेब सर्वर या एप्लीकेशन में अंतर्निहित है और एप्लीकेशन पर लॉग इन करने में सक्षम करने के लिये व्यापक संख्या में कंपनियों द्वारा इसका उपयोग किया जाता है।
    - 'जावा' (Java) दुनिया में सबसे अधिक इस्तेमाल की जाने वाली प्रोग्रामिंग भाषाओं में से एक है।
- यह सुभेद्यता 'Log4j 2' संस्करणों, जो दुनिया भर में उपयोग की जाने वाली एक बहुत ही कॉमन लॉगिंग लाइब्रेरी है, को प्रभावित करता है।
    - लॉगिंग, डेवलपर्स (Developers) को एक एप्लीकेशन की सभी गतिविधियों को देखने की अनुमति देता है।
- एप्पल (Apple), माइक्रोसॉफ्ट (Microsoft), गूगल (Google) जैसी सभी टेक कंपनियाँ इस ओपन-सोर्स लाइब्रेरी (Open-Source Library) पर भरोसा करती हैं, जैसा कि एंटरप्राइज़ एप्लीकेशन सिस्को (CISCO), नेटएप (Netapp), क्लाउडफेयर (Cloudflare),
- अमेज़न (Amazon) और अन्य पर करते हैं।

गंभीर/सीवियर रेटिंग (Severe Rating):

- Log4Shell को सुरक्षा विशेषज्ञों द्वारा इसे 10 की गंभीर/सीवियर रेटिंग दी गई है।
- यह सुभेद्यता एक हैकर को सिस्टम पर नियंत्रण करने की अनुमति दे सकती है।
    - एक साइबर हमलावर उपभोक्ता द्वारा प्रति या किसी फाइल में लॉगिंग करने हेतु दी गई कमॉन्ड के समय लॉगिंग वाले सर्वर को हैक कर सकता है।
    - यह एक बुनियादी "प्रति" निर्देश को लीक-सम-सीक्रेटे-डेटा-आउट-ऑन-ओंट-द--इंटरनेट सिचुएशन (Leak-Some-Secret-Data-Out-Onto-The-Internet Situation) या डाउनलोड-एंड-रन-माय-मैलवेयर-एट-वन्स कमांड (Download-And-Run-My-Malware-At-Once Command) में परिवर्तित कर सकता है।
    - सरल शब्दों में कहें, तो कानूनी या सुरक्षा कारणों से किया गया एक लॉग **मैलवेयर** आरोपण घटना (Malware Implantation Event) में परिवर्तित हो सकता है।

रिमोट कोड निष्पादन (RCE):

- एक पंक्ति के कोड का उपयोग करके भेद्यता का फायदा उठाया जा सकता है जो हमलावरों को पीड़ित के सिस्टम पर रिमोट कमांड निष्पादित करने की अनुमति देता है।
- किसी भी जावा-आधारित वेब सर्वर को नियंत्रित करने और रिमोट कोड निष्पादन (Remote Code Execution-RCE) हमलों को अंजाम देने के लिये हमलावरों द्वारा इसका उपयोग किया जा सकता है।
- RCE हमले में हमलावर लक्षित प्रणाली पर नियंत्रण कर लेते हैं और अपनी इच्छानुसार कोई भी कार्य कर सकते हैं।
- कई रिपोर्टों के अनुसार, इस भेद्यता पर पहले से ही हैकर द्वारा परीक्षण किया जा रहा है, और यह उन्हें एक एप्लीकेशन तक पहुँच प्रदान करता है, जो संभावित रूप से उन्हें डिवाइस या सर्वर पर दुर्भावनापूर्ण सॉफ्टवेयर चलाने की अनुमति प्रदान करता है।

Log4Shell भेद्यता का प्रभाव:

- **क्रिप्टोकरेंसी माइनिंग:** उनके द्वारा महसूस किये गए अधिकांश हमले पीड़ितों की कीमत पर क्रिप्टोकरेंसी माइनिंग के उपयोग पर केंद्रित प्रतीत होते हैं। हालाँकि मूल शोषण के नए रूपांतरण तेजी से पेश किये जा रहे हैं।
    - इस भेद्यता के सफल दोहन से संवेदनशील जानकारी का खुलासा हो सकता है, डेटा में वृद्धि या संशोधन हो सकता है, या सेवा से इनकार (DoS) हो सकता है।
- **वैश्विक:** इससे ऑस्ट्रेलिया-न्यूज़ीलैंड (ANZ) क्षेत्र सबसे अधिक प्रभावित क्षेत्र था जिसमें 46% कॉर्पोरेट नेटवर्क एक प्रयास के शोषण का सामना कर रहे थे।
    - जबकि इस तरह के प्रयास का सामना करने वाले 36.4% संगठनों के साथ उत्तरी अमेरिका सबसे कम प्रभावित था।
- **भारत:** भारत में लगभग 41% कॉर्पोरेट नेटवर्क पहले ही शोषण के प्रयास का सामना कर चुके हैं।
    - भारतीय कंपनियाँ अपने पश्चिमी समकक्षों की तुलना में अधिक असुरक्षित नहीं हैं क्योंकि वे जावा-आधारित अनुप्रयोगों का उपयोग करती हैं।
    - भारतीय कंपनियाँ अपनी कमज़ोर सुरक्षा स्थिति के कारण उच्च जोखिम में हैं, विशेष रूप से छोटी कंपनियाँ जिनके पास समस्या का पता लगाने और उसे जल्दी से ठीक करने के लिये जानकारी या संसाधन नहीं हो सकते हैं।

स्रोत-इंडियन एक्सप्रेस