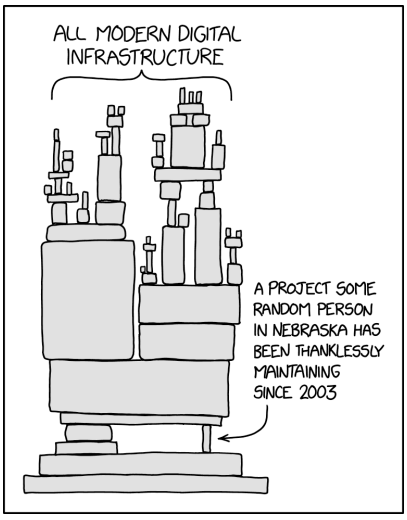
CVE-2024-3094: XZ Utils Backdoor

Descrizione degli eventi:

XZ Utils è un set di strumenti open-source per la compressione dati utilizzati di default su molte distribuzioni Linux. Il 29 marzo 2024, Andres Freund, ricercatore presso Microsoft, ha scoperto che le versioni 5.6.0 di XZ Utils contenevano un backdoor che permetteva ad attaccanti remoti non autenticati di eseguire codice arbitrario sui sistemi vulnerabili, bypassando l'autenticazione SSH.

XZ Utils è un software che mette a disposizione una libreria (libzma) utilizzata da molti progetti per la compressione e decompressione di file. In particolare, la falla sfruttava la sua rilevanza all'interno di Systemd (libsystemd) e OpenSSH.



L'introduzione del backdoor è stata un'operazione complessa, attuata nell'arco di tre anni da un utente di GitHub chiamato JiaT75 (Jia Tan) con l'aiuto di altri account fittizi. Tan è riuscito gradualmente a guadagnare la fiducia dei manutentori e a impiantare il codice malevolo nei test della libreria.

Il backdoor sfrutta vulnerabilità nel codice dei test per iniettare uno script che decomprime ed esegue un oggetto binario contenente il payload vero e proprio. Questo payload sostituisce la funzione RSA_decrypt di OpenSSH per verificare ed eseguire comandi firmati con una chiave privata dell'attaccante.

Sebbene non ci siano prove di sfruttamento attivo, CVE-2024-3094 ha una gravità massima (CVSS 10.0) perché abilita l'esecuzione remota di codice come utente del servizio SSH. Per essere vulnerabili, i sistemi devono eseguire Linux x86/64, avere le versioni compromesse di XZ Utils installate tramite un gestore pacchetti ed esporre SSH su Internet.

L'impatto della vulnerabilità è stato minimo grazie alla scoperta di Freund, ma sarebbe potuto essere uno degli incidenti più gravi della storia della sicurezza informatica.

Attacchi alla supply chain

L'incidente ha evidenziato i rischi degli attacchi alla supply chain nell'open source e la necessità di maggiori controlli sulle dipendenze critiche, spesso gestite solo da pochi volontari.

Da anni si registrano aumenti degli attacchi diretti ai progetti open source e ai comparti IT delle aziende a livello locale e internazionale. A questi si aggiungono interdipendenze sempre più complesse che rendono difficile la gestione della sicurezza.

Invece che infettare progetti open source con una migliore gestione e un maggior controllo delle patch sottomesse dai diversi contributori, è stata preferita un'operazione di ingegneria sociale per introdurre un backdoor in un progetto minore alla base di diversi sistemi come Systemd e OpenSSH.

Soluzioni al problema?

Quando ci sono eventi di questa portata come la CVE-2024-3094, è comune vedere molte discussioni su come si sarebbe potuto evitare l'incidente. Difficilmente ci si concentra sulle cause più profonde che hanno portato alla vulnerabilità e all'ingegneria sociale che ha permesso l'introduzione del backdoor, e invece ci si prolunga in discussioni infinite su quale potesse essere la pipeline di lavoro che avrebbe potuto evitare la vulnerabilità.

Alla base di questa CVE-2024-3094 è presente uno dei problemi più comuni all'interno dell'open source: piccoli progetti sostenuti e mantenuti da poche persone diventano la base di sistemi complessi sviluppati da società e organizzazioni di grandi dimensioni, senza però una adeguata gestione del rischio e un diretto sovvenzionamento tramite finanziamenti diretti o indiretti.

Finché si farà affidamento, senza adeguato finanziamento e gestione del rischio, sui single point of failure, sarà sempre più comune trovare vulnerabilità come CVE-2024-3094.

Riferimenti

- CVE-2024-3094
- Ubuntu Security Notice
- Report Pentest tools