CVE Report for Kali Linux

CVE-2024-3094: xz-utils Backdoor

CVE-2024-3094 è una vulnerabilità rilevante che ha interessato Kali Linux e altre distribuzioni Linux. Questa vulnerabilità ha coinvolto la libreria xz-utils, utilizzata per la compressione dei dati, nelle versioni 5.6.0 e 5.6.1.
La problematica ha permesso la potenziale compromissione dei sistemi tramite una backdoor che ha facilitato accessi remoti non autorizzati.

Dettagli del CVE:

- Descrizione: Iniezione di codice dannoso in xz-utils che permetteva attacchi remoti.
- Impatto: Potenziale compromissione del sistema e accesso remoto non autorizzato.
- Versioni affette: xz-utils 5.6.0-0.2 a 5.6.1-1.
- Risoluzione: L'aggiornamento a una versione più sicura, come la 5.4.5, ha eliminato la vulnerabilità.

Istruzioni per il controllo e l'aggiornamento:

1. Verifica la versione di liblzma5:

```
$ apt-cache policy liblzma5
```

2. Aggiorna se necessario:

```
$ sudo apt update && sudo apt install -y --only-upgrade liblzma5
```

Lezioni apprese:

Questo incidente evidenzia l'importanza di un monitoraggio costante delle vulnerabilità e della prontezza nel rispondere agli aggiornamenti di sicurezza.

Fonti:

- Cybersecurity News

- JFrog Security Insights

- Openwall e Help Net Security