Uno strano bug di Linux consente l'invio di comandi root

Ott 16, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Basta inserire un ID particolare per elevare i privilegi di un utente a root. Per fortuna la falla riguarda solo i sistemi con (improbabili) impostazioni personalizzate.

Secondo i ricercatori di sicurezza, il bug individuato in **Linux** non dovrebbe creare troppi problemi a livello globale. Nonostante riguardi una tecnica che permette di elevare i privilegi di un utente, infatti, la falla di sicurezza (CVE-2019-14287) è stata infatti classificata da **Red Hat** con uno score di "solo" **7.8** su 10.

Il motivo? Un eventuale exploit funziona solo se l'amministratore ha impostato la funzione Sudo (quella che consente di avere privilegi di super utente – ndr) per consentire a qualsiasi utente all'interno di un gruppo l'esecuzione di comandi come se fosse un altro utente.

L'impostazione, che può essere inserita nel file **sudoers** che regola l'uso di Sudo, consente in pratica di concedere a tutti gli utenti la possibilità di controllare gli altri utenti (con l'eccezione del super user) utilizzando **RunAs**.

Nelle intenzioni, quindi, una impostazione di questo genere consente un ampio campo di azione, ma esclude i privilegi di root. **Peccato che le cose non funzionino esattamente così**.

Se un utente esegue un comando impostando l'ID utente con il valore -1 (il comando completo è **sudo -u#-1**), infatti, acquisisce automaticamente i privilegi di root. Il valore -1, infatti, viene interpretato come "non cambiare l'ID dell'utente". **E visto che Sudo viene avviato come root, il sistema esegue il comando con i massimi privilegi**.

L'elemento curioso è che lo stesso accade se si usa il comando **-u#4294967295**, che in 32 bit corrisponde proprio a -1. Il bug è stato prontamente corretto con il rilascio di Sudo **1.8.28**. Ci si aspetta, quindi, che tutti gli aggiornamenti per le varie distro lo includano.

La speranza, in ogni caso, è che i sistemi potenzialmente vulnerabili siano pochi, se non pochissimi. La stessa idea di permettere a qualsiasi utente di eseguire qualsiasi comando come se fosse un altro, da un punto di vista logico, è piuttosto bizzarra.

Condividi l’articolo

Apple aiuta la Cina a tracciare gli utenti? No, però…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/16/uno-strano-bug-di-linux-consente-linvio-di-comandi-root/