Backdoor in OpenSSH Server gefunden

Eine Backdoor (CVE-2024-3094) in XZ Utils könnte einem Angreifer erlauben, die OpenSSH Server Authentifizierung zu brechen.

Die Libary XZ Utils, welche unter Umständen vom OpenSSH Server verwendet wird, wurde in Version 3.6 kompromittiert und enthält eine backdoor.

Der Microsoft-Softwareingenieur Andres Freund entdeckte das Sicherheitsproblem, als er langsame SSH-Anmeldungen auf einer Linux-Maschine unter Debian Sid (der aktuellen Entwicklungsversion der Debian-Distribution) untersuchte. In den XZ Utils Datenkompressionswerkzeugen und -Bibliotheken wurde ein Backdoor gefunden. Die Lücke wird unter der Bezeichnung CVE-2024-3094 behandelt. Der entsprechende Bugreport ist als Issue auf Github zu finden.

Red Hat hat heute empfohlen, Systeme mit Fedora-Entwicklungs- und Experimentalversionen sofort herunterzufahren. OpenSSH Server verwendet liblzma nicht direkt. Debian und einige andere Distributionen patchen jedoch openssh, um Systemd-Benachrichtigungen zu unterstützen und libsystemd verwendet liblzma.

Betroffene Linux Distributionen mit OpenSSH Server backdoor

Vom Backdoor in OpenSSH Betroffen sind unter anderem Debian Unstable und testing. Reguläre Debian Releases wie z.B. Debian Bookworm sind nach aktuellen Stand nicht betroffen. RHEL ist nicht betroffen, allerdings warnt Red Hat vor der Verwendung von aktuellen Fedora Rawhide Installationen:

Auf Github kursiert ein script, mit welchem die Sicherheit des eigenen Systems überprüft werden kann.