Inhalt

Über eine **Lücke im Cryptsetup** gelangt man kinderleicht in eine Shell, in der man Kommandos mit Root-Rechten ausführen kann. Wenn man diese Nachricht liest, mag man zunächst glauben, dass hier extrem stümperhaft gearbeitet wurde. Einfach 70 Sekunden lang die Eingabe-Taste betätigen, und schon hat man Zugriff auf das verschlüsselte System. Vorsicht mit schnellen Urteilen!

Wo ist die Ursache und was sind die Konsequenzen?

Ursache für Lücke im Cryptsetup *

Sicherheitslücke Cryptsetup

Es ist nicht etwa so, dass ein **Timer** prüft, wie lange die Enter-Taste gedrückt wird und dann nach Ablauf von 70 Sekunden die **Root Shell** öffnet. Das könnte man dann eventuell sogar als mutwilliges Einbringen einer **Backdoor** bezeichnen. Die Ursache ist, wie so oft, komplexer. Das Betätigen der Eingabetaste ruft eine Routine zum Überprüfen des eingegebenen Passworts auf. Drückt man auf die Entertaste, sendet die Taste regelmäßig das Kommando „Eingabe“. In 70 Sekunden etwa 95 Mal. Anscheinend ist es auf zahlreichen Linux-Systeme so, dass der Anwender genau diese (*es sollen 93 sein*) Versuche hat, das korrekte Passwort beim Booten einzugeben.

Sind all diese Eingaben falsch, dann geschieht das, was eben nicht passieren sollte. Es wird eine allgemeine Fehlerbehandlung aufgerufen, die als letzte Rettungsmaßnahme

eine Root Shell öffnet.

Hätte man statt dieses Maximalwerts 93 eine **Endlosschleife** programmiert die bis zur Eingabe des korrekten Passwortes durchlaufen wird, gäbe es keine Lücke.

Konsequenzen der Cryptsetup Lücke *

Es sei klar gestellt, dass man die Entertaste bis zum jüngsten Tag drücken kann und trotzdem kein Zugriff auf die verschlüsselten Daten im Klartext möglich wäre. Zum Entschlüsseln wird das korrekte Passwort benötigt, daran führt kein Weg vorbei.

Was droht denn dann? Bringt man das System dazu, neu zu starten, dann kann man durch betätigen der Eingabetaste und 70 Sekunden Geduld in den oben beschriebenen Zustand versetzen.

Eine mögliche Maßnahme eines Angreifers könnte jetzt sein, die Daten der verschlüsselten Partitionen zu kopieren und sich später in Ruhe darum zu kümmern. Dies halte ich, bei Einhaltung bestimmter Prinzipien bei der Passwortwahl für relativ unkritisch.

Wesentlich schwerwiegender ist die Möglichkeit, das System zu manipulieren und etwa Schadsoftware zu installieren, die ab jetzt einfach die Passworteingabe protokolliert.

Legt es der Angreifer rein auf **Sabotage** aus, hat er ein leichtes Spiel. Über die Root-Shell ist es ein Kinderspiel, das System zu vernichten.

Weitere Informationen...

Bildnachweis:
Stockfoto-ID: 132586811
Copyright: Chitsanupong

