Kernel-Panik


Achim Leitner, stellv. Chefredakteur

Wenn Linux im Sturzflug gerade noch „Oops“ schreit und sich dann mit einer Kernel Panic ins Daten-Nirwana verabschiedet, bricht bei den Admins kollektives Stirnrunzeln aus: Linux stürzt ja nicht ab, und wenn doch, ist meist die Hardware schuld. Oder es sind Cracker am Werk, die ihren dreckigen Job – glücklicherweise – unsauber erledigen.

Letzteres erlebte das Debian-Projekt an den eigenen Servern: Über das abgehörte Passwort eines Users und einen Kernel-Exploit installierten Eindringlinge ein Rootkit. Kernel-Oopse auf mehreren Maschinen schreckten die Betreiber auf.

Suckit hat den Angreifer verraten – selbstverständlich unfreiwillig, denn die (zweifelhafte) Aufgabe eines Rootkits ist es ja, jede Enttarnung zu verhindern und dem Cracker dauerhaft Zugang zum System zu verschaffen. Trickreich modifiziert Suckit einen laufenden Kernel, nistet sich in dessen Innereien ein und versteckt seine Aktionen vor den Kommandos der Admins. Gut für die Administratoren: Suckit scheint sich nicht mit dem verwendeten Debian-Kernel zu vertragen und provozierte die Abstürze. Ein weiterer Glücksfall: Dieses Rootkit versteckt zwar Files, aber es hat die Änderungen an »/sbin/init« nicht vor dem Integritätsprüfer AIDE verborgen. So konnte dieses Tool die Manipulation bemerken und melden.

So deutlich gewarnt begannen fähige Debian-Jünger mit einer eingehenden forensischen Analyse. Dabei stießen sie auf eine interessante Hinterlassenschaft der Eindringlinge: einen verschleierten Root-Exploit (per Burneye-Code-Obfuscation getarnt). Wieder ein Glücksfall: Der eilends zusammengeballten Kraft der Mitarbeiter von Suse, Red Hat und Debian hielt der Schutz nicht Stand. Der entschlüsselte Exploit offenbarte eine Sicherheitslücke im Kernel, von der außer den Bösewichten bis dato offenbar niemand wusste.

Interessanterweise war im aktuellen Kernel 2.4.23 und auch im 2.6.0-test6 diese Lücke bereits geschlossen – nur ahnte wohl niemand, welche Auswirkungen der unscheinbare Integer-Überlauf im »do_brk()«-Syscall haben könnte. Wegen der Tragweite sind die Kernelentwickler dann vermutlich selbst in Kernel-Panik verfallen.

Im Ergebnis hat der Vorfall der Linux-Gemeinde mehr geholfen als geschadet: Wissen aus dem Untergrund über eine gravierende Sicherheitslücke sickerte an die Oberfläche. Sie wurde gestopft und verantwortungsvolle Admins können ihre Maschinen jetzt abdichten. Dieses Ergebnis hätte der Cracker auch leichter haben können: Mit einer E-Mail an die Bugtraq-Liste. Dann könnte er jetzt auch öffentlich Lob für seine Entdeckung ernten und wäre nicht mit dem Makel belegt, die Zeit der Debian-Entwickler geraubt zu haben.