



Linux ptrace Root Exploit

by Ivan Buetler
ivan.buetler@csnc.ch

Linux ptrace() Root Exploit

27. März 2003

Einführung

Am 23. März 2003 ist ein „local root exploit“ für Linux publiziert worden. Dieser Linux Exploit ist daher besonders erwähnenswert, da er für die Kernel 2.2.x bis 2.4.x anwendbar ist. Damit sind die Linux Kernel der letzten 2 Jahre betroffen!

Der Exploit verschafft einem niedrig privilegiertem User administrative Berechtigungen und ist äusserst einfach zu bedienen.

```
hobo@poas:~> pwd
/home/hobo

hobo@poas:~> id
uid=119(hobo) gid=139(csnc)

hobo@poas:~> ./ptrace-get-root

sh-2.05# id
uid=0(root) gid=0(root)
sh-2.05#
```

Beim obigen Test führt der niedrig privilegierte Benutzer „hobo“ den Exploit aus und wird damit „root“.

Beschreibung der Sicherheitslücke

Wenn ein Prozess auf Funktionen zugreift, die in Linux Kernelmodulen implementiert sind, dann wird dafür ein Child-Prozess eröffnet.

Dieser Child-Prozess setzt das euid und egid auf 0 und ruft („/sbin/modprobe“) durch execve auf.

Das Grundproblem liegt nun darin begründet, dass ein Hacker sich durch die Funktion ptrace() an den Child Prozess „attachen“ kann, bevor das euid (effektive UID) auf 0 gesetzt wird. Diese Attacke wird im Fachjargon als „race condition“ bezeichnet. Damit kann der Angreifer eigenen Code ins Memory des Zielprozesses kopieren, der dann unter root Privilegien abläuft.

Jeder User besitzt unter Unix zur „reellen“ UID und GID die „effektiven“ EUID und seine EGID, die benutzt werden, um erweiterte Zugriffsrechte auf Dateien in spezifischen Fällen zu realisieren.

Zunächst sind die reellen Werte und die effektiven identisch, letztere können bei Bedarf jedoch kurzfristig geändert werden um auf speziell geschützte Dateien Zugriff zu erlangen. So ist es zum Beispiel möglich, als „normaler“ User das eigene Passwort zu ändern (suid flag).

Voraussetzungen für Hacker

Damit diese Sicherheitslücke ausgenutzt werden kann, müssen folgende Bedingungen erfüllt sein:

- Der Kernel unterstützt loadable Modules (kein monolithischer Kernel)
- Das File /proc/sys/kernel/modprobe enthält mindestens einen Eintrag zu einem real existierenden Binary im Filesystem
- ptrace() calls sind erlaubt

Die obigen Bedingungen sind bei den meisten Linux Installationen erfüllt.

Was ist ptrace?

Die Linux Funktion ptrace() erlaubt dem „parent prozess“ den „child prozess“ zu überwachen und kontrollieren. Es handelt sich um eine Diagnose Funktion.

```
MANUAL PTRACE
ptrace() provides tracing and debugging
facilities. It allows one process (the
tracing process) to control another (the
traced process). Most of the time, the
traced process runs normally, but when it
receives a signal (see sigaction(2)), it
stops. The tracing process is expected to
notice this via wait(2) or the delivery of a
SIGCHLD signal, examine the state of the
stopped process, and cause it to terminate
or continue as appropriate. ptrace() is the
mechanism by which all this happens.
```



Linux ptrace Root Exploit

by Ivan Buetler
ivan.buetler@csnc.ch

Lösungsansätze

Für die Lösung dieser Sicherheitslücke bieten sich folgende Methoden an:

- Kernel Patch
- Disable kmod/module
- Installation von ptrace-blocking modul
- Modifikation /proc/sys/kernel/modprobe derart, dass auf ein ungültiges File gezeigt wird

Der Kernel 2.5 ist gemäss heutigen Erkenntnissen von der Sicherheitslücke **nicht** betroffen. Der Kernel 2.5 startet modprobe durch keventd, welcher unter einer non-root uid läuft.

Praxisbezug – Apache Webserver

Wir möchten davor warnen, dass diese Sicherheitslücke bald in einem Wurm vorkommen könnte. Der bekannte NIMDA Wurm hat ebenfalls auf einer Sicherheitslücke basiert, der in der Security Branche bereits länger bekannt war.

Im Labor der Compass Security hat der Exploit sowohl auf Linux Systemen funktioniert, die auf Standard-Kernels basieren, als auch auf selbst kompilierten Kernels.

Bei der ptrace Sicherheitslücke handelt es sich um einen „Local Exploit“. Dieser ist über das Netzwerk nicht anwendbar. Wir gehen aber davon aus, dass zukünftige Linux Exploits den ptrace Exploit beinhalten.

Nehmen wir zum Beispiel an, dass in Zukunft eine Linux Apache Sicherheitslücke bekannt wird, die das Ausführen von Malicious Mobile Code erlaubt (siehe OpenSSL Bug). Der ptrace Exploit könnte demnach dem Apache Prozess zu administrativen Privilegien verhelfen und Grundlage für weit gefährlichere Attacken und Würmer darstellen.

Aus diesem Grund empfehlen wir die gegenüber dem Internet sichtbaren Dienste zusätzlich einem Hardening zu unterziehen. Bei der Testinstallation von Compass Security hat ein in der CHROOT befindlicher Prozess keine Möglichkeit auf /sbin/modprobe zuzugreifen. Als eine weitere Schutzmöglichkeit für die Verhinderung eines zukünftigen Wurmes sehen wir:

- CHROOT'ing des Services
- File Permissions derart setzen, dass ein Zugriff auf /sbin/modprobe unterdrückt wird

Referenzen

SUSE LINUX:

http://www.suse.de/de/security/2003_21_kernel.html

SECURITYFOCUS:

<http://www.securityfocus.com/bid/2529>

CERT:

<http://www.kb.cert.org/vuls/id/176888>

HEISE Security Ticker

<http://www.heise.de/newsticker/data/ju-26.03.03-000/>

Kontakt

Ivan Bütler ist Geschäftsführer der Compass Security AG, ein auf Penetration Test und Security Review spezialisiertes Schweizer Unternehmen.

Compass Security AG
Ivan Bütler
Postfach 1671
CH-8640 Rapperswil

ivan.buetler@csnc.ch
<http://www.csnc.ch>