

Dienstag, 15. September 2009

## **FreeBSD: Zero-Day-Exploit unter FreeBSD 6 und 7**

Wie nun bekannt wurde gibt es unter FreeBSD 6.0 bis FreeBSD 6.4 und auch FreeBSD 7.2 einen 0-day-root-exploit welcher bis dato noch nicht behoben wurde. Auch ist eine offizielle Stellungnahme seitens des FreeBSD Projects bis jetzt nicht bekannt.

Wie der Entdecker der Schwachstelle, Frasunek, mitteilte, hat er das FreeBSD Project bereits am 29. August 2009 darüber in Kenntnis gesetzt. Robert Watson, einer der FreeBSD Core Team member, teilte mit, dass die E-Mail "lost in a slew" ist und er davon ausgeht, dass es in Kürze ein offizielles advisory geben wird.

Bei der Schwachstelle handelt es sich um einen lokalen zero-day-exploit. Das heisst, ein Anwender muss Zugriff auf das System haben um root-Rechte zu erlangen.

Laut The Register ist Version 7.1 und später nicht betroffen, allerdings zeigt dieses Video, dass auch FreeBSD 7.2 betroffen ist.

Laut dem Entdecker der Schwachstelle ist es sehr einfach die Schwachstelle auszunutzen, welche anscheinend mit kqueue zusammenhängt.

Videos:

FreeBSD 6.x Exploit

FreeBSD 7.2 Exploit

Weitere Informationen:

The Register

UPDATE:

Wie ich eben in der Mailingliste gelesen habe, ist das FreeBSD Security Team dabei einen Patch zu testen.

Xin Li schreibt dazu:

Currently we (secteam@) are testing the correction patch and do peer-review on the security advisory draft, the bug was found and fixed on -HEAD and 7-STABLE before 7.1-RELEASE during some stress test but was not recognized as a security vulnerability at that time. The exploit code has to be executed locally, i.e. either by an untrusted local user, or be exploited in conjunction with some remote vulnerability on applications that allow the attacker to inject their own code.

We can not release further details about the problem at this time, though, but I think we will likely to publish the advisory and correction patch this patch Wednesday.

Es wird also in Kürze mit einem Patch gerechnet.

Geschrieben von asg in Security um 09:18