

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

### Im Interview: Daniel Seuffert bei Pofacs zu DesktopBSD

Nach der Sommerpause geht es bei Pofacs direkt mit BSD weiter. Diesmal ist Daniel Seuffert im Interview (mittlerweile schon Podcast Nummer 59) mit Pofacs und berichtet über DesktopBSD.

Dem Podcast kann direkt über die Internetseite von Pofacs gelauscht werden. Ein MP3 und OGG gibt es ebenfalls zum download.

Weitere Informationen:

<http://www.desktopbsd.net>

<https://portal.bsdgroup.de/>

<http://de.wikipedia.org/wiki/DesktopBSD>

[http://de.wikipedia.org/wiki/Berkeley\\_Software\\_Distribution](http://de.wikipedia.org/wiki/Berkeley_Software_Distribution)

[http://de.wikipedia.org/wiki/ZFS\\_\(Dateisystem\)](http://de.wikipedia.org/wiki/ZFS_(Dateisystem))

Geschrieben von asg in Interviews um 09:02

### **DesktopBSD: So long, and thanks for all the fish**

Es war in letzter Zeit ziemlich ruhig geworden um DesktopBSD, doch nun ist doch eine neue Version von DesktopBSD erschienen, DesktopBSD 1.7.

Dies wird allerdings auch die letzte Version von DesktopBSD von Peter Hofer, dem Entwickler, sein.

Zu den Änderungen gehören dabei:

FreeBSD 7.2 as stable and secure base system

KDE 3.5.10 as mature and easy-to-use desktop environment

OpenOffice.org 3.1.1 as feature-rich office suite

Pre-installed Java SE 6 environment

X.Org release 7.4 with extensive graphics hardware support

Large number of enhancements and fixes

Den Download gibt es hier.

Neben PCBSD ist DesktopBSD die wohl bekannteste und älteste Version von FreeBSD welche die Nutzung von FreeBSD für den Desktop vereinfacht. Im Gegensatz zu PCBSD wird DesktopBSD allerdings mehr oder weniger von einer Person, Peter Hofer, entwickelt. Da ein solches Projekt, um auch immer auf dem aktuellen Stand zu bleiben, viel Zeit benötigt, hat Peter nun einen Schlusstrich gezogen:

This is the last and final release of the DesktopBSD project. I find myself having less and less time to spare lately and no longer desire to keep developing and maintaining this project. However, because DesktopBSD is based entirely on FreeBSD, further support for the operating system and availability of up-to-date software for DesktopBSD 1.7 is ensured.

Ob sich hier eventuell andere Entwickler finden, welche das Projekt weiterführen, ist nicht bekannt. Nutzer von DesktopBSD werden, da DesktopBSD auf FreeBSD aufsetzt, durch FreeBSD mit Updates versorgt, allerdings ist die Entwicklung, Stand heute, von DesktopBSD abgeschlossen und wird nicht weiter verfolgt.

Danke an Peter Hofer, welcher, durch die Entwicklung von DesktopBSD, FreeBSD für den Desktop besser nutzbar machte, was gerade Anfänger sehr zu schätzen wussten.

Geschrieben von asg in FreeBSD um 08:30

Montag, 14. September 2009

## **BSDCertification wird Professional**

Die BSDCertification Group arbeitet im Hintergrund unermüdlich am BSDP Examen. Dieses wird, aller Voraussicht nach, im ersten Quartal 2010 erscheinen. Um das BSDP Examen zu machen bedarf es keiner BSDA Zertifizierung.

Bevor die BSDCertification Group allerdings das Examen anbieten kann, ist die Hilfe der Community gefragt. Hierbei geht es, wie schon bei den Vorbereitungen zum BSDA Examen, um eine Umfrage hinsichtlich der Themen welche beim BSDP Examen keinesfalls fehlen sollten und welche in der Community einen hohen Stellenwert haben.

Die Umfrage ist hier zu finden. Nehmt Euch bitte 20 bis 30 Minuten Zeit, je mehr an der Umfrage teilnehmen um so besser kann das BSDP Examen später ausfallen und die Forderungen der Community an ein BSD Examen widerspiegeln. Danke.

Das BSDP Examen ist für BSD Sysadmins welche schon einige Jahre Erfahrung mit der Administration von BSD Systemen haben.

Sollten Fragen zur Umfrage (JTA Survey) aufkommen so kann die BSDCertification Group direkt angeschrieben werden.

Weitere Informationen:

<http://www.bsdcertification.org/>

<http://bsdcg.blogspot.com/>

<http://wiki.bsdcertificationgroup.org/bsdcert/Translations>

<http://www.facebook.com/group.php?gid=55432547309>

<http://www.linkedin.com/groups?gid=1600807>

<http://www.linkedin.com/groups?gid=1600767>

Geschrieben von asg in BSD-CG um 13:18