Admins - Anomalie #1817

CVE-2016-5195

24/10/2016 17:00 - Christian P. Momon

Statut:	Fermé	**Début:**	24/10/2016
Priorité:	Immédiate	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Il semble que la faille CVE-2016-5195 ne soit pas corrigé sur les machines du SI de l'April :

https://security-tracker.debian.org/tracker/CVE-2016-5195

indique que :

```
jessie    3.16.36-1+deb8u1    vulnerable
```

Or :

```
cpm@ocmstar (16:58:42) ~/Dossiers/April/Adminsys/git/scripts 9 > ./do.sh uname -a |grep -v ===
Linux bastion 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux admin 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux dns 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux mail 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux sympa 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux adl 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux lamp 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux agir 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux bots 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux dtc 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux drupal6 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux republique-numerique 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/L
inux
Linux mumble 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux candidatsbe 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux candidatsfr 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux pad 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux scm 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux virola.april.org 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
Linux calamus.april.org 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linu
x
Linux galanga 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86_64 GNU/Linux
```

J'en conclue qu'il faut une mise à jour et un reboot de toutes les machines.

Plus d'infos sur la faille :

http://www.generation-nt.com/dirty-cow-vulnerabilite-linux-actualite-1934759.html

Cela me pousse à penser que c'est urgent.

Historique

#1 - 25/10/2016 00:09 - Christian P. Momon

Celui qui a trouvé la faille a écris :

http://arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/

```
Less trivially, any web server/application vulnerability which allows the attacker to upload a file to the imp
```

```
acted system and execute it also works.
```

Avec le recul, je me dis que j'ai peut-être lu un peu trop vite. Avons-nous une application web qui exécute des upload ? La correction est importante mais peut-être pas urgente.

Autre article :
http://www.nextinpact.com/news/101856-une-faille-dans-kernel-linux-vieille-9-ans-corrigee-mais-deja-exploitee.htm

#2 - 25/10/2016 09:49 - François Poulain

Ce genre de vulnérabilité n'est pas très impactante si elle est isolée dans un SI qui ne fournit pas de shell au premier venu. Mais couplée à un mécanisme d'injection de code, elle est très sérieuse. Et perso si je devais estimer si le SI de l'April est vulnérable ou non aux exécutions arbitraire de code, je pencherais pour un oui. :)

#3 - 31/10/2016 09:16 - François Poulain

- Statut changé de Nouveau à Fermé

A priori on est désormais en 3.16.36-1+deb8u2 partout sauf sur opium et scopo. Donc la faille est bouchée.

Pour opium, un reboot est prévu par benj quand il sera au local.

Pour scopo, je vais vérifier que l'update est bien configuré (il ne l'ait visiblement pas donc je vais corriger), mais vu les services hébergés ce n'est pas un gros soucis pour moi.

#4 - 31/10/2016 09:24 - François Poulain

Ha beh non: scopo est juste en oldstable. Elle est à jour mais son kernel est vulnérable.

#5 - 04/12/2020 22:15 - Christian P. Momon

- Assigné à mis à François Poulain