Journal : demain soir on finit tard

Posté par **Trollnad Dump** le 16/10/18 à 23:50. **Licence CC by-sa.**
Tags : **libssh**, **faille**, **cve-2018-10933**, **ssh**

Le CVE 2018-10933 concernant la **libssh** est limpide : demain on reporte tout à après demain et à la place on fait les mises à jour (si si, même pour toi le petit serveur du fond de la classe qui ne fait jamais ses mises à jour à cause de *(place ici une mauvaise excuse)*)

```
bonjour server
bonjour
je voudrais avoir un accès
vous avez besoin d'un mot de passe, $user
mais je n'en ai aucun !
OK ! Bienvenue $user
```

0.8.4 & 0.7.6 sont disponibles dans toutes les bonnes crèmeries.

Bonne journée à vous aussi !

https://www.libssh.org/2018/10/16/libssh-0-8-4-and-0-7-6-security-and-bugfix-release/

Plus tard

Posté par **nigaiden** le 17/10/18 à 00:16. Évalué à 8 (+7/-0).

D'après ce que lis, libssh est un projet indépendant de OpenSSH. Bien entendu, il y a des **applications impactées**, mais cela ne veut pas dire non plus que tous les serveurs SSH sont troués.

Re: Plus tard

Posté par **Trollnad Dump** le 17/10/18 à 00:28. Évalué à 5 (+3/-0). Dernière modification le 17/10/18 à 00:33.

Oui, d'où le lien dans le journal sous libssh vers wikibook.

Pas de version patchée dans Debian Security?

Posté par **jihele** le 17/10/18 à 09:27. Évalué à 2 (+0/-0).

> *0.8.4 & 0.7.6 sont disponibles dans toutes les bonnes crèmeries.*

Dans Debian, pas de 0.7.6 et 0.8.4 attendra 5 jours comme tout le monde.

https://tracker.debian.org/pkg/libssh
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=911149

Ça devrait pas passer dans stable-security, ça ?

Re: Pas de version patchée dans Debian Security?

Posté par **Arthur Accroc** le 17/10/18 à 14:25. Évalué à 4 (+3/-1). Dernière modification le 17/10/18 à 14:25.

> > *0.8.4 & 0.7.6 sont disponibles dans toutes les bonnes crèmeries.*
>
> *Dans Debian, pas de 0.7.6 et 0.8.4 attendra 5 jours comme tout le monde.*

Les « bonnes crèmeries », ce sont celles qui ont de la crème *fraîche*, non ?

> Théorie du pot-au-feu : « tout milieu où existe une notion de hauteur (notamment les milieux économique, politique, professionnels) se comporte comme un pot-au-feu : les mauvaises graisses remontent. »

Re: Pas de version patchée dans Debian Security?

Posté par **StyMaar** le 17/10/18 à 15:14. Évalué à 5 (+4/-0).

> *Les « bonnes crèmeries », ce sont celles qui ont de la crème fraîche, non ?*

Oui, mais paradoxalement la «crème fraîche» c'est de la crème (légèrement) fermentée ;)

Re: Pas de version patchée dans Debian Security?

Posté par **CrEv** (**page perso**) le 18/10/18 à 09:48. Évalué à 2 (+0/-0).

> *Les « bonnes crèmeries », ce sont celles qui ont de la crème fraîche, non ?*

Et moi qui croyait que c'était là où on trouve de bonnes glaces 🅲 🅰

Re: Pas de version patchée dans Debian Security?

Posté par **Benoit Sibaud** (**page perso**) le 18/10/18 à 20:40. Évalué à 8 (+5/-0). Dernière modification le 18/10/18 à 20:40.

https://www.debian.org/security/2018/dsa-4322 (et **https://security-tracker.debian.org/tracker/DLA-1548-1** pour le LTS Jessie)
d'où le statut **https://security-tracker.debian.org/tracker/CVE-2018-10933**

Lien vers le CVE

Posté par **freem** le 17/10/18 à 09:31. Évalué à 2 (+0/-0). Dernière modification le 17/10/18 à 09:31.

Le **lien** vers la CVE semble impliquer que cette faille ne concerne «que»

> *A flaw was found in python-cryptography versions between >=1.9.0 and <2.3.*

Par contre, ce que je ne comprend pas (mais ce n'est pas la première fois que j'ai du mal à comprendre les numéro de version de paquets Debian... faudra que je creuse un jour), dans Debian les versions que j'ai (en stable + backports) sont potentiellement "0.7.3" et "0.8.1", ça semble loin de 1.9.0? D'ailleurs il n'y a pas de Mâj de sécu dispo à l'heure ou j'écrit ces lignes... j'aurai tendance à en déduire que Debian n'est pas affectée?

Re: Lien vers le CVE

Posté par **Jihele** le 17/10/18 à 10:04. Évalué à 7 (+5/-0). Dernière modification le 17/10/18 à 10:05.

`>=1.9.0` and `<2.3` , c'est les versions de python-cryptography, pas celles de libssh.

https://tracker.debian.org/pkg/libssh

stable: 0.7.3-2
stable-bpo: 0.8.1-1~bpo9+1
testing: 0.8.1-1
unstable: 0.8.4-2

Pour le reste, j'ai les mêmes interrogations.

Quant à python-cryptography, on dirait bien que Debian est passée entre les gouttes :

https://tracker.debian.org/pkg/python-cryptography

stable: 1.7.1-3
testing: 2.3-1
unstable: 2.3-1

Re: Lien vers le CVE

Posté par **AnCaRioN** le 17/10/18 à 11:33. Évalué à 2 (+2/-0). Dernière modification le 17/10/18 à 11:36.

C'est python-cryptography qui est en 1.7.1 sous stretch et 2.3 sous sid.

libssh est bien dans les branches 0.7.* et 0.8.*

Ps : j'ai été devancé :x

Re: Lien vers le CVE

Posté par **Eric P.** (**page perso**) le 19/10/18 à 13:06. Évalué à 3 (+2/-0).

Le lien que tu donnes est pour pour la faille **CVE-2018-10903** dans une lib python.
Le journal s'interesse a la faille **CVS-2018-10933** qui est dans libssl.

> Excusez l'absence d'accents dans mes commentaires, j'habite en Allemagne et n'ai pas de clavier francais sous la main.

Re: Lien vers le CVE

Posté par **Xavier Claude** (**page perso**) le 19/10/18 à 13:48. Évalué à 3 (+0/-0).

s/l\./h./

> « Rappelez-vous toujours que si la Gestapo avait les moyens de vous faire parler, les politiciens ont, eux, les moyens de vous faire taire. » Coluche

ou pas

Posté par **steph1978** le 18/10/18 à 19:26. Évalué à 6 (+5/-1).

On parle d'une bibliothèque indépendante de openssh.
Qui permet de faire des applications clientes ou serveurs.
Quand je la cherche le la trouve que sur mon poste de dev.
Donc ne concerne pas la majorité des déploiements de SSH, loin de là ; plutôt une minorité.
Ne concerne pas que les serveurs.
Pas de quoi y passer la soirée.

Aucun serveur impacté

Posté par **brendel** le 18/10/18 à 20:29. Évalué à 4 (+3/-0).

IIRC la personne qui a reporté la CVE à elle-même indiqué qu'elle n'avait pas trouvé d'implémentation serveur utilisant la libssh, uniquement client. Donc à priori tous les serveurs un minimum utilisés ne sont pas impactés.

Re: Aucun serveur impacté

Posté par **Sufflope** (**page perso**) le 18/10/18 à 21:31. Évalué à 2 (+1/-1).

Cocasse venant de quelqu'un véhiculant un message politique dans son pseudo DLFP d'utiliser le même artifice que sa cible (les *fake news* pour faire trembler dans les chaumières).

Re: Aucun serveur impacté

Posté par **Pressper** le 18/10/18 à 22:26. Évalué à 6 (+4/-0).

Pourtant, y avait pas a chercher bien loin **https://www.libssh.org/features/**

Who uses libssh?
[...]
***GitHub** implemented **their git ssh server** with libssh*
[...]

Re: Aucun serveur impacté

Posté par **lamdmdlsr** le 19/10/18 à 06:48. Évalué à 2 (+1/-0).

Who uses libssh?

[...]
csync a bidirectional file synchronizer
[...]

Sauf erreur de ma part, Nextcloud et Owncloud utilisent csync, non ?

Re: Aucun serveur impacté

Posté par **Firwen** (**page perso**) le 19/10/18 à 11:49. Évalué à 3 (+1/-0).

> *Sauf erreur de ma part, Nextcloud et Owncloud utilisent csync, non ?*

Ils l'utilisent(-aient ? je suis plus sur que c'est d'actualité) pour la synchronization bidirectionnel sur WebDAV. Rien à voir avec SSH.

Note : les commentaires appartiennent à ceux qui les ont postés. Nous n'en sommes pas responsables.