

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

CAIS-Alerta [18/10/2018]: Vulnerabilidade na biblioteca LIBSSH

O CAIS alerta para a recente vulnerabilidade encontrada na biblioteca libssh, utilizada em algumas implementações do protocolo SSHv2 em aplicações cliente e servidor.

DESCRIÇÃO

A vulnerabilidade encontra-se no código utilizado no lado servidor e permite o usuário burlar o processo de autenticação de modo que seja mantido o estado de conexão autenticada permitindo, até mesmo, a criação novos canais entre cliente e servidor. Para que isso ocorra, um cliente malicioso envia ao servidor remoto uma mensagem "SSH2_MSG_USERAUTH_SUCCESS" no lugar da mensagem "SSH2_MSG_USERAUTH_REQUEST", assim o servidor permite o acesso sem exigência das credencias.

SISTEMAS IMPACTADOS

Sistemas utilizando aplicações baseadas na libssh.

VERSÕES AFETADAS

Versão 0.6 e superiores da biblioteca libssh.

CORREÇÕES DISPONÍVEIS

Atualizar a versão da biblioteca libssh para a mais recente disponível conforme recomendação dos mantenedores ou versão mais atual recomendada para o seu ambiente.

IDENTIFICADORES CVE (<http://cve.mitre.org>)

CVE-2018-10933

MAIS INFORMAÇÕES

- [1] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-10933>
- [2] <https://www.libssh.org/security/advisories/CVE-2018-10933.txt>
- [3] <https://nvd.nist.gov/vuln/detail/CVE-2018-10933>

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os alertas do CAIS também podem ser acompanhados pelas redes sociais da RNP. Siga-nos!

Twitter: @RedeRNP

Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

```
#####  
# CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS) #  
# Rede Nacional de Ensino e Pesquisa (RNP) #  
# #  
# cais@cais.rnp.br http://www.rnp.br/servicos/seguranca #  
# Tel. 019-37873300 Fax. 019-37873301 #  
# Chave PGP disponivel https://www.cais.rnp.br/cais-pgp.key #  
#####
```

```
-----BEGIN PGP SIGNATURE-----  
Version: OpenPGP.js v1.0.1  
Comment: http://openpgpjs.org
```

```
wsFcBAEBCAAQBQJbyNFtCRB83qA0uPj0mAAARK8QAKQSQKm01Kd0GN92vJqA  
eVHACIZjSfxqpj1Qe3DfsuxACHEFMEQC0bgzyXsBmtPtXTqo7JXCfEv9S1zs  
Qy0a3mG6PfJ5AEBOnYFBwu11F1ut/IFKZpL0q+XNsSpYQ7H+NMbwX/ySRoLD  
ymZqh4UgBZ45+OrbdRsuF9j6Dqx8hM4+SuKNygEHYxq1pSNv4aXQ9w1Mbmhh  
8RQs61Dxf4doypy1SYWPiZYJKVVKZJYrjF27jTs0Tc1z4o+pduKW1THhqqb/  
aDz128dpuU/pgw31Ztf8I1rng9TM6IL2XtCVd1aKd0Ts0NBqVw1RxCsaRQEu  
9f0DHXXiCdBCqFTI8t1Iu7cZWVON4Ah7gCZLn7TRN9fvwc/FZkBjBd5kuPZh  
0KsJeQ09c1Die1Vm7wXXy7S+Nu9T1sXB9Qj+OpjxrXSkaliTQDJxwkJEbmE+  
NtxEwSv8Pyogo1EhHgbEsxDK/oFnuXhQpeb1BM7/rKqGYUe3AIsjNNp+RI0b  
vzeap4cRkp0UBpv3caNXSy5t4WeJnoHzbfRrVPrsUHSc7VmNBHS9k1yKkeKb  
cFLs6tqqqheSBuPtBFefjAz7edqdzw51aX0s0VQN4KcFSrtXNxITa09C0Yca  
AyXfNF5Kp+gj/W5dU3e7o6ASsig3g7A31Yaxoa5+15fYvC/pVw1PxdlDwj+D  
FENI
```

```
=9YU4
```

```
-----END PGP SIGNATURE-----
```