

S . G . D . S . N
Agence nationale
de la sécurité des
systèmes d'information

Paris, le 21 juillet 2021
N° CERTFR-2021-AVI-553

Affaire suivie par: CERT-FR

AVIS DU CERT-FR

Objet: Multiples vulnérabilités dans le noyau Linux de Debian

GESTION DU DOCUMENT

| | |
|-----------------------------|--|
| Référence | CERTFR-2021-AVI-553 |
| Titre | Multiples vulnérabilités dans le noyau Linux de Debian |
| Date de la première version | 21 juillet 2021 |
| Date de la dernière version | 21 juillet 2021 |
| Source(s) | Bulletin de sécurité Debian dla-2714 du 20 juillet 2021 Bulletin de sécurité Debian dla-2713-2 du 20 juillet 2021 Bulletin de sécurité Debian dla-2713 du 20 juillet 2021 Bulletin de sécurité Debian dsa-4941 du 20 juillet 2021 |
| Pièce(s) jointe(s) | Aucune(s) |

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

RISQUE(S)

- Dénî de service
- Atteinte à la confidentialité des données
- Élévation de privilèges

SYSTÈMES AFFECTÉS

- Debian buster versions antérieures à 4.19.194-3
- Debian 9 stretch versions antérieures à 4.9.272-2
- Debian 9 stretch versions antérieures à 4.19.194-3~deb9u1

RÉSUMÉ

De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian et Debian LTS. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges.

SOLUTION

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION

- Bulletin de sécurité Debian dla-2714 du 20 juillet 2021
<https://www.debian.org/lts/security/2021/dla-2714> (<https://www.debian.org/lts/security/2021/dla-2714>)
- Bulletin de sécurité Debian dla-2713-2 du 20 juillet 2021
<https://www.debian.org/lts/security/2021/dla-2713-2> (<https://www.debian.org/lts/security/2021/dla-2713-2>)
- Bulletin de sécurité Debian dla-2713 du 20 juillet 2021
<https://www.debian.org/lts/security/2021/dla-2713> (<https://www.debian.org/lts/security/2021/dla-2713>)
- Bulletin de sécurité Debian dsa-4941 du 20 juillet 2021
<https://www.debian.org/security/2021/dsa-4941> (<https://www.debian.org/security/2021/dsa-4941>)
- Référence CVE CVE-2020-36311
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36311> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36311>)
- Référence CVE CVE-2021-3609
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3609> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3609>)
- Référence CVE CVE-2021-33909
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909>)
- Référence CVE cve-2021-33909

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-33909> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-33909>)

- Référence CVE CVE-2021-34693

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34693> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34693>)

- Référence CVE CVE-2021-21781

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21781> (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21781>)

GESTION DÉTAILLÉE DU DOCUMENT

le 21 juillet 2021

Version initiale
