Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

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

Paris, le 17 juin 2022
N° CERTFR-2022-AVI-567

Affaire suivie par: CERT-FR

AVIS DU CERT-FR

Objet: Multiples vulnérabilités dans le noyau Linux de SUSE

Gestion du document

Référence	CERTFR-2022-AVI-567
Titre	Multiples vulnérabilités dans le noyau Linux de SUSE
Date de la première version	17 juin 2022
Date de la dernière version	17 juin 2022
Source(s)	Bulletin de sécurité le noyau Linux de SUSE suse-su-20222103-1 du 16 juin 2022 Bulletin de sécurité le noyau Linux de SUSE suse-su-20222104-1 du 16 juin 2022
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)

- Exécution de code arbitraire
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Élévation de privilèges

Systèmes affectés

- SUSE Enterprise Storage 7
- SUSE Linux Enterprise High Availability 15
- SUSE Linux Enterprise High Availability 15-SP2
- SUSE Linux Enterprise High Performance Computing 15
- SUSE Linux Enterprise High Performance Computing 15-ESPOS
- SUSE Linux Enterprise High Performance Computing 15-LTSS
- SUSE Linux Enterprise High Performance Computing 15-SP2
- SUSE Linux Enterprise High Performance Computing 15-SP2-ESPOS
- SUSE Linux Enterprise High Performance Computing 15-SP2-LTSS
- SUSE Linux Enterprise Module for Live Patching 15
- SUSE Linux Enterprise Module for Live Patching 15-SP2
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 15-LTSS
- SUSE Linux Enterprise Server 15-SP2
- SUSE Linux Enterprise Server 15-SP2-BCL
- SUSE Linux Enterprise Server 15-SP2-LTSS
- SUSE Linux Enterprise Server for SAP 15
- SUSE Linux Enterprise Server for SAP 15-SP2
- SUSE Linux Enterprise Server for SAP Applications 15
- SUSE Linux Enterprise Server for SAP Applications 15-SP2
- SUSE Manager Proxy 4.1
- SUSE Manager Retail Branch Server 4.1
- SUSE Manager Server 4.1

Résumé

De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité.

Contournement provisoire

Solution

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

Documentation

- Bulletin de sécurité le noyau Linux de SUSE suse-su-20222103-1 du 16 juin 2022
  https://www.suse.com/support/update/announcement/2022/suse-su-20222103-1/
- Bulletin de sécurité le noyau Linux de SUSE suse-su-20222104-1 du 16 juin 2022
  https://www.suse.com/support/update/announcement/2022/suse-su-20222104-1/
- Référence CVE CVE-2022-21127
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21127
- Référence CVE CVE-2022-21123
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21123
- Référence CVE CVE-2022-21125
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21125

- Référence CVE CVE-2022-21180
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21180
- Référence CVE CVE-2022-21166
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21166
- Référence CVE CVE-2019-19377
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19377
- Référence CVE CVE-2022-1184
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1184
- Référence CVE CVE-2017-13695
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13695
- Référence CVE CVE-2022-1729
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1729
- Référence CVE CVE-2022-1652
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1652
- Référence CVE CVE-2021-39711
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39711
- Référence CVE CVE-2022-1419
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1419
- Référence CVE CVE-2021-43389
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43389
- Référence CVE CVE-2021-38208
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38208
- Référence CVE CVE-2022-1353
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1353
- Référence CVE CVE-2021-20292
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20292
- Référence CVE CVE-2022-1011
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1011
- Référence CVE CVE-2022-1974
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1974
- Référence CVE CVE-2022-1975
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1975
- Référence CVE CVE-2022-21499
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21499
- Référence CVE CVE-2022-1734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1734
- Référence CVE CVE-2022-30594
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30594
- Référence CVE CVE-2021-33061
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33061
- Référence CVE CVE-2022-1516
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1516
- Référence CVE CVE-2021-20321
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20321
- Référence CVE CVE-2019-20811
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20811
- Référence CVE CVE-2022-0168
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0168
- Référence CVE CVE-2022-1966
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1966
- Référence CVE CVE-2022-28893
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28893
- Référence CVE CVE-2022-1158
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1158
- Référence CVE CVE-2020-26541
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26541

Gestion détaillée du document

le 17 juin 2022

Version initiale