ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans SUSE Linux Kernel
Numéro de Référence	58531411/25
Date de Publication	14 Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Basesystem Module 15-SP7
- Development Tools Module 15-SP7
- Legacy Module 15-SP7
- SUSE Linux Enterprise Desktop 15 SP7
- SUSE Linux Enterprise High Availability Extension 15 SP7
- SUSE Linux Enterprise High Performance Computing 12 SP5
- SUSE Linux Enterprise High Performance Computing 15 SP3
- SUSE Linux Enterprise High Performance Computing 15 SP4
- SUSE Linux Enterprise High Performance Computing 15 SP5
- SUSE Linux Enterprise Live Patching 12-SP5
- SUSE Linux Enterprise Live Patching 15-SP3
- SUSE Linux Enterprise Live Patching 15-SP4
- SUSE Linux Enterprise Live Patching 15-SP5
- SUSE Linux Enterprise Live Patching 15-SP6
- SUSE Linux Enterprise Live Patching 15-SP7
- SUSE Linux Enterprise Micro 5.1
- SUSE Linux Enterprise Micro 5.2
- SUSE Linux Enterprise Micro 5.3
- SUSE Linux Enterprise Micro 5.4
- SUSE Linux Enterprise Micro 5.5
- SUSE Linux Enterprise Real Time 15 SP4
- SUSE Linux Enterprise Real Time 15 SP5
- SUSE Linux Enterprise Real Time 15 SP6
- SUSE Linux Enterprise Real Time 15 SP7
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 15 SP3
- SUSE Linux Enterprise Server 15 SP4

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- SUSE Linux Enterprise Server 15 SP5
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server 15 SP7
- SUSE Linux Enterprise Server for SAP Applications 12 SP5
- SUSE Linux Enterprise Server for SAP Applications 15 SP3
- SUSE Linux Enterprise Server for SAP Applications 15 SP4
- SUSE Linux Enterprise Server for SAP Applications 15 SP5
- SUSE Linux Enterprise Server for SAP Applications 15 SP6
- SUSE Linux Enterprise Server for SAP Applications 15 SP7
- SUSE Linux Enterprise Workstation Extension 15 SP7
- openSUSE Leap 15.3
- openSUSE Leap 15.4
- openSUSE Leap 15.5
- openSUSE Leap 15.6

Identificateurs externes

- CVE-2022-2586 CVE-2022-3640 CVE-2022-50212 CVE-2022-50213
- CVE-2022-50248 CVE-2023-42753 CVE-2023-53247 CVE-2023-53252
- CVE-2023-53287 CVE-2023-53333 CVE-2023-53338 CVE-2023-53368
- CVE-2023-53377 CVE-2023-53515 CVE-2023-53638 CVE-2023-53699
- CVE-2024-53197 CVE-2025-21756 CVE-2025-38212 CVE-2025-38539
- CVE-2025-38685 CVE-2025-38702 CVE-2025-39721 CVE-2025-39726
- CVE-2025-39730 CVE-2025-39732 CVE-2025-39743 CVE-2025-39757
- CVE-2025-39790 CVE-2025-39810 CVE-2025-39824 CVE-2025-39841
- CVE-2025-39849 CVE-2025-39850 CVE-2025-39851 CVE-2025-39860
- CVE-2025-39861 CVE-2025-39863 CVE-2025-39864 CVE-2025-39866
- CVE-2025-39869 CVE-2025-39873 CVE-2025-39907 CVE-2025-39923
- CVE-2025-39925 CVE-2025-39945 CVE-2025-39952 CVE-2025-39967
- CVE-2025-39968 CVE-2025-39970 CVE-2025-39971 CVE-2025-39972
- CVE-2025-39973 CVE-2025-39978 CVE-2025-39981 CVE-2025-39982
- CVE-2025-39985 CVE-2025-39986 CVE-2025-39987 CVE-2025-39988
- CVE-2025-39994 CVE-2025-39996 CVE-2025-40000 CVE-2025-40037
- CVE-2025-40091 CVE-2025-40096

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans SUSE Linux Kernel. Un attaquant à distance pourrait exploiter certaines de ces vulnérabilités pour causer un déni de service, réussir une élévation de privilège, exécuter du code arbitraire à distance et de divulguer des informations confidentielles sur le système ciblé. SUSE confirme que les deux vulnérabilités (CVE-2022-2586 et CVE-2024-53197) sont activement exploitées.

Solution

Veuillez se référer au bulletin de sécurité SUSE du 12 Novembre 2025, afin d'installer les nouvelles mises à jour.

Risque

- Déni de service
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité de données
- Elévation de privilèges

Référence

Bulletin de sécurité SUSE du 12 Novembre 2025:

- https://www.hkcert.org/security-bulletin/suse-linux-kernel-multiple-vulnerabilities_20251103