ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le noyau de SUSE Linux
Numéro de Référence	59730601/26
Date de publication	06 janvier 2026
Risque	Important
Impact	Important

Systèmes affectés

- Public Cloud Module 15-SP7
- SUSE Enterprise Storage 7.1
- SUSE Linux Enterprise High Availability Extension 15 SP3
- SUSE Linux Enterprise High Availability Extension 15 SP4
- 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 ESPOS 15 SP4
- SUSE Linux Enterprise High Performance Computing LTSS 15 SP3
- SUSE Linux Enterprise High Performance Computing LTSS 15 SP4
- 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-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 for Rancher 5.2
- SUSE Linux Enterprise Micro for Rancher 5.3
- SUSE Linux Enterprise Micro for Rancher 5.4
- SUSE Linux Enterprise Real Time 15 SP4

- SUSE Linux Enterprise Real Time 15 SP6
- SUSE Linux Enterprise Real Time 15 SP7
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 12 SP5 LTSS
- SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security
- SUSE Linux Enterprise Server 15 SP3
- SUSE Linux Enterprise Server 15 SP3 Business Critical Linux
- SUSE Linux Enterprise Server 15 SP3 LTSS
- SUSE Linux Enterprise Server 15 SP4
- SUSE Linux Enterprise Server 15 SP4 LTSS
- 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 SP6
- SUSE Linux Enterprise Server for SAP Applications 15 SP7
- SUSE Manager Proxy 4.2
- SUSE Manager Proxy 4.3
- SUSE Manager Proxy 4.3 LTS
- SUSE Manager Retail Branch Server 4.2
- SUSE Manager Retail Branch Server 4.3
- SUSE Manager Retail Branch Server 4.3 LTS
- SUSE Manager Server 4.2
- SUSE Manager Server 4.3
- SUSE Manager Server 4.3 LTS
- SUSE Real Time Module 15-SP6
- SUSE Real Time Module 15-SP7
- openSUSE Leap 15.3
- openSUSE Leap 15.4
- openSUSE Leap 15.6

Identificateurs externes

CVE-2022-50253	CVE-2022-50280	CVE-2022-50364	CVE-2022-50368	CVE-2022-50494
CVE-2022-50545	CVE-2022-50551	CVE-2022-50569	CVE-2022-50578	CVE-2023-53229
CVE-2023-53369	CVE-2023-53431	CVE-2023-53542	CVE-2023-53597	CVE-2023-53641
CVE-2023-53659	CVE-2023-53676	CVE-2023-53717	CVE-2025-21710	CVE-2025-37916
CVE-2025-38359	CVE-2025-38360	CVE-2025-38361	CVE-2025-38436	CVE-2025-39788
CVE-2025-39805	CVE-2025-39819	CVE-2025-39822	CVE-2025-39859	CVE-2025-39944
CVE-2025-39967	CVE-2025-39980	CVE-2025-40001	CVE-2025-40021	CVE-2025-40027
CVE-2025-40030	CVE-2025-40038	CVE-2025-40040	CVE-2025-40047	CVE-2025-40048
CVE-2025-40055	CVE-2025-40059	CVE-2025-40064	CVE-2025-40070	CVE-2025-40074
CVE-2025-40075	CVE-2025-40080	CVE-2025-40083	CVE-2025-40086	CVE-2025-40098

CVE-2025-40105	CVE-2025-40107	CVE-2025-40109	CVE-2025-40110	CVE-2025-40111
CVE-2025-40115	CVE-2025-40116	CVE-2025-40118	CVE-2025-40120	CVE-2025-40121
CVE-2025-40127	CVE-2025-40129	CVE-2025-40139	CVE-2025-40140	CVE-2025-40141
CVE-2025-40149	CVE-2025-40154	CVE-2025-40156	CVE-2025-40157	CVE-2025-40159
CVE-2025-40164	CVE-2025-40168	CVE-2025-40169	CVE-2025-40171	CVE-2025-40172
CVE-2025-40173	CVE-2025-40176	CVE-2025-40180	CVE-2025-40183	CVE-2025-40185
CVE-2025-40186	CVE-2025-40188	CVE-2025-40194	CVE-2025-40198	CVE-2025-40200
CVE-2025-40204	CVE-2025-40205	CVE-2025-40206	CVE-2025-40207	

Bilan de la vulnérabilité

SUSE annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant le noyau de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder à des données confidentielles ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de SUSE afin d'installer les nouvelles mises à jour.

Risques

- Contournement de mesures de sécurité
- Accès à des données confidentielles
- Déni de service

Références

Bulletin de sécurité de SUSE :

- https://www.suse.com/support/update/announcement/2025/suse-su-20254515-1
- https://www.suse.com/support/update/announcement/2025/suse-su-20254516-1
- https://www.suse.com/support/update/announcement/2025/suse-su-20254517-1

- https://www.suse.com/support/update/announcement/2025/suse-su-20254521-1
- https://www.suse.com/support/update/announcement/2025/suse-su-20254530-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260029-1

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma