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	61570203/26
Date de publication	03 mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- openSUSE Leap 15.4
- openSUSE Leap 15.5
- openSUSE Leap 15.6
- SUSE Linux Enterprise High Performance Computing 12 SP5
- 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-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 5.3
- 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 11 SP4
- SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 15 SP4
- 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 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

Identificateurs externes

CVE-2021-0920 CVE-2022-50700 CVE-2022-50717 CVE-2023-54142 CVE-2025-38129 CVE-2025-38177

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 d'exécuter du code à distance, d'accéder à des données confidentielles, d'élever ses privilèges, de contourner des mesures de sécurité 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
- Contournement de mesures de sécurité
- Elévation de privilèges
- Déni de service

Références

Bulletin de sécurité de SUSE :

- https://www.suse.com/support/update/announcement/2026/suse-su-20260674-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260688-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260696-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260698-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260700-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260707-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260710-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260711-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260713-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260725-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260727-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260731-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260734-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260736-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260745-1
- https://www.suse.com/support/update/announcement/2026/suse-su-20260748-1

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma