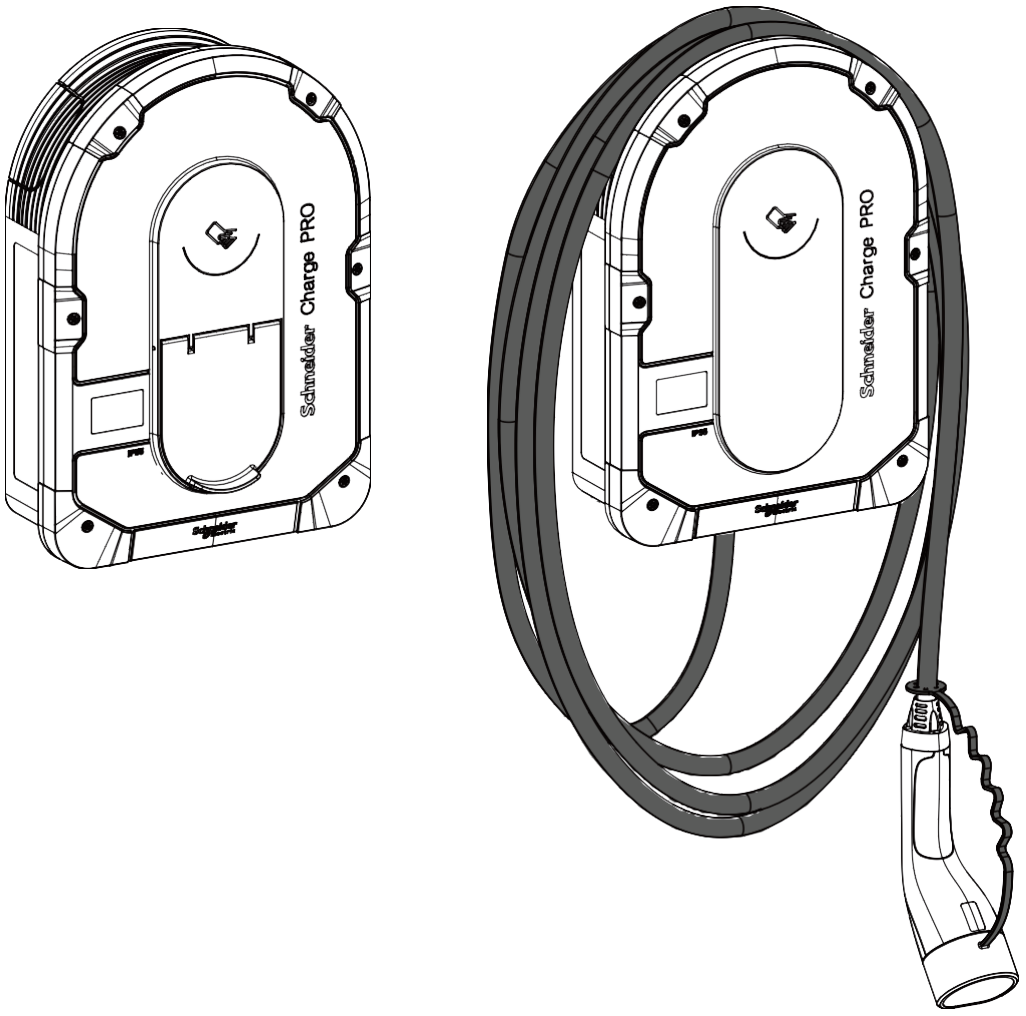
Schneider Charge Pro

Manuel de cybersécurité

BRU5883000-02_FR

04/2025



www.se.com

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Les équipements électriques doivent être installés, exploités et entretenus par un personnel qualifié. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de cet appareil.

Table des Matières

Sécurité Informations **4**
Consignes de sécurité 5
A propos **6**
Informations relatives à la cybersécurité **7**
La cybersécurité au sein de Schneider Electric **8**
Politiques de cybersécurité 8
Ressources en matière de cybersécurité 8
Solutions de Cybersécurité 8
Portail d'assistance à la Cybersécurité 8
Caractéristiques de sécurité 9
Protocoles pris en charge 10
Risques éventuels et contrôles compensatoires 10
Conseils de sécurité **11**
Recommandations pour la mise en service 11
Code PIN par défaut 11
Sécurité de la communication OCPP 11
Sécurité de SSDP 11
Configuration des services 12
Conseils de sécurité pour le fonctionnement 12
Mise à jour du micrologiciel 12
Journal d'audit 12
Conseils de sécurité en cas de mise hors service 12
Réinitialisation aux paramètres d'usine 12
Annexe A **13**
Logiciels libres utilisés dans le Schneider Charge Pro 13

Sécurité Informations

Informations importantes

Lisez ces instructions attentivement et examinez l'équipement pour vous familiariser avec l'appareil avant d'essayer de l'installer, de le faire fonctionner ou d'en effectuer l'entretien. Les messages spéciaux suivants peuvent apparaître dans cette documentation ou sur l'équipement pour avertir de dangers potentiels ou pour attirer l'attention sur des informations qui clarifient ou simplifient une procédure.

L'ajout de ce symbole à une étiquette de sécurité « Danger » ou « Avertis-sement » dénote l'existence d'un risque électrique susceptible de provoquer des blessures corporelles si les instructions ne sont pas respectées.

Ceci est le symbole d'alerte de sécurité. Il est utilisé pour vous avertir des risques potentiels de blessures. Respectez tous les messages de sécurité qui suivent ce symbole afin de prévenir tout risque de blessure ou de décès.

⚠ DANGER

DANGER indique une situation dangereuse qui, si elle n'est pas évitée, **causera la mort** ou des blessures graves.

⚠ AVERTISSEMENT

AVERTISSEMENT indique une situation dangereuse qui, si elle n'est pas évitée, **peut entraîner** la mort ou des blessures graves.

⚠ ATTENTION

ATTENTION indique une situation dangereuse qui, si elle n'est pas évitée, **peut entraîner** des blessures mineures ou modérées.

AVIS

AVIS est utilisé pour aborder des pratiques qui ne sont pas liées à des blessures physiques.

Veuillez Noter

Les équipements électriques doivent être installés, exploités et entretenus par un personnel qualifié. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de cet appareil.

Une personne qualifiée s'entend comme une personne dotée de compétences et de connaissances en rapport avec la construction et le fonctionnement du matériel électrique ainsi que son installation, et disposant d'une formation adéquate en matière de sécurité lui permettant d'identifier et d'éviter les risques encourus.

Consignes de sécurité

⚠ DANGER

RISQUE DE CHOC ÉLECTRIQUE
- Il ne faut pas ouvrir l'appareil.
- Seul un personnel qualifié est habilité à effectuer l'entretien du produit.

Tout manquement à ces instructions peut entraîner la mort ou des blessures graves.

REMARQUE : Il convient de respecter toutes les instructions applicables au produit joint ainsi que toutes les précautions de sécurité.

Pour en savoir plus, il vous est possible de télécharger l'application du Centre d'assistance à la clientèle en utilisant le code QR suivant :

A propos

Objectif de ce document

La borne de recharge Schneider Charge Pro prend en charge la connexion à des réseaux Ethernet/WIFI, bien que sa capacité de mise en réseau ne soit pas conçue pour résister à l'exposition directe à l'Internet public.

La borne de recharge Schneider Charge Pro a vocation à fonctionner dans un environnement réseau sécurisé, par exemple derrière des pare-feu, et/ou dans les limites d'un réseau OT isolé (séparé du réseau IT).

Note de validité

Ce document porte sur les bornes de recharge Schneider Charge Pro.

Terminologie

Acronyme	Désignation
OCPP	Open Charge Point Protocol (protocole de communication établi entre les bornes de recharge et un système central)

Informations relatives à la cybersécurité

Informations importantes

⚠ AVERTISSEMENT

RISQUES POUVANT AFFECTER LA DISPONIBILITÉ, DE L'INTÉGRITÉ ET DE LA CONFIDENTIALITÉ DU SYSTÈME

- Il faut d'abord modifier les mots de passe par défaut en vue d'empêcher l'accès non autorisé aux paramètres, aux commandes et aux informations de l'appareil.
- En désactivant les ports/services inutilisés et les comptes par défaut, on réduit les voies d'accès pour les attaquants malveillants.
- Connectez les appareils au réseau en utilisant de multiples niveaux de cyberdéfense (pare-feu, segmentation du réseau, détection et protection contre les intrusions dans le réseau, etc.)
- Respectez les bonnes pratiques de cybersécurité (par exemple, le principe du moindre privilège, la séparation des tâches) pour réduire les risques d'intrusion, la perte ou l'altération des données et des journaux, ou l'interruption des services.

Tout manquement à ces instructions risque de conduire à la mort, à des blessures graves ou à l'endommagement du dispositif.

La cybersécurité au sein de Schneider Electric

La cybersécurité est au coeur de la stratégie de Schneider Electric, qui suit une posture de cybersécurité couvrant de nombreux aspects :

- La sécurisation des activités internes
- La protection renforcée des systèmes et actifs informatiques stratégiques
- La conduite de la transformation numérique en respectant le cadre de la cybersécurité.
- La conception et le développement de nouveaux produits et solutions intégrant des mesures de cybersécurité et de protection de bout en bout.

Politiques de cybersécurité

Schneider Electric suit un cycle de développement sécurisé (SDL) conforme à la norme de sécurité IEC 62443-4-1 pour les systèmes d'automatisation et de contrôle industriels afin de soutenir le développement et la maintenance des produits.

Ce cycle consiste à mettre en oeuvre un processus qui s'appuie sur les bonnes pratiques en matière de sécurité et sur des outils dédiés :

- Former à la cybersécurité les équipes impliquer dans la conception, ect la conception, du développement et de l'essai des produits.
- Analyse du modèle de menace et revue de sécurité de la conception
- Analyse de code statique et revue de sécurité du code
- Tests de penetration et tests de vulnérabilités périodiques
- Un processus rigoureux de gestion des vulnérabilités

Ressources en matière de cybersécurité

Solutions de Cybersécurité

Pour obtenir des recommandations et des conseils pour améliorer la sécurité de l'environnement et de l'infrastructure dans lesquel Schneider Charge Pro est déployé, Schneider Electric publies des lignes directrives, des livres blancs et des bonnes pratiques qui peuvent être consultés sur la page Solutions de Cybersécurité du site web mondial de Schneider Electric.

Portail d'assistance à la Cybersécurité

Il existe en outre d'autres ressources disponibles sur le Portail d'assistance à la Cybersécurité de Schneider Electric, parmi lesquelles

- la politique de gestion des vulnérabilités de Schneider Electric
- Les notifications de sécurité au sujet des vulnérabilités affectant les produits et les systèmes

La politique de gestion des vulnérabilités de Schneider Electric aborde les vulnérabilités de cybersécurité qui affectent sur les produits de Schneider Electric dans le but de contribuer à la sécurité et à la sûreté de nos clients.

En collaboration avec les chercheurs, soit on garde le terme anglais qui est aussi utilisé communément en français soit je propose “centre d'alerte et de réaction aux attaques informatiques” et les propriétaires d'installations, Schneider Electric veille à ce que des informations exactes soient fournies en temps utile afin de protéger correctement les installations de ses clients.

Le Corporate Product CERT (CPCERT) de Schneider Electric a pour mission à la fois la gestion et l'alerte en cas de vulnérabilités et de mesures d'atténuation affectant les produits.

Le Portail d'assistance à la Cybersécurité offre également des interfaces de signalement des vulnérabilités à supprimer et vous facilite l'inscription à la liste de diffusion des mises à jour des notifications de sécurité afin de vous tenir informé par courrier électronique des notifications de sécurité nouvellement publiées ou actualisées.

Caractéristiques de sécurité

La borne de recharge Schneider Charge Pro intègre des caractéristiques de sécurité afin de garantir que le produit fonctionne conformément à l'usage auquel il est destiné.

Il s'agit de fonctions de sécurité qui sont censées protéger le produit contre les menaces potentielles pouvant perturber le fonctionnement du produit (disponibilité), en modifier la configuration (intégrité) ou divulguer des informations (confidentialité).

En voici les caractéristiques principales :

- Contrôle de l'authenticité du micrologiciel au démarrage du produit (démarrage sécurisé)
- Mise à jour du micrologiciel avec vérification de la signature du micrologiciel (à l'aide de la cryptographie asymétrique)
- TLS 1.2 pour la sécurisation et l'authentification des communications OCPP avec un à supprimer système de gestion de la borne de recharge (CSMS).
- Puce de sécurité certifiée Critères communs EAL6+ permettant de sauvegarder la clé privée et le certificat du produit.
- La désactivation des interfaces internes de débogage et de test.

Ces caractéristiques de sécurité servent à atténuer les menaces inhérentes à la mise en œuvre des bornes de recharge Schneider Charge Pro au sein de l'environnement pour lequel elles ont été conçues.

Leur efficacité dépend toutefois de la mise en œuvre et de la bonne application des recommandations figurant dans le présent guide pour la mise en service, l'exploitation et la maintenance des bornes de recharge Schneider Charge Pro, ainsi que des Meilleures Pratiques Recommandées en Matière de Cybersécurité.

Protocoles pris en charge

Les protocoles mentionnés ci-dessous sont supportés avec les bornes de recharge Schneider Charge Pro :

Protocole	Utilisation
OCPP (TLS 1.2) + HTTPS/FTPS	Communications à distance au système de gestion de la borne de recharge **REMARQUE :** Le protocole OCPP repose sur des communications HTTPS/FTPS supplémentaires visant à prendre en charge les rapports OCPP et les opérations de maintenance (mise à jour du micrologiciel).
HTTPS (TLS 1.2)	Configuration par le biais d'outils de configuration
Modbus RTU	Communications aux centrales de mesure de la puissance
DHCP	Adresse IP pour le réseau
DNS	Résolution des noms de réseau
ISO/IEC 14443A/B ISO/IEC 15693	Authentification des utilisateurs à l'aide de badges RFID
SSDP	Protocole simple de découverte de services (Simple Service Discovery Protocol)

Risques éventuels et contrôles compensatoires

Domaine	Enjeu	Risque	Contrôles compensatoires
Accès physique	Il est possible qu'une borne de recharge fasse l'objet de tentatives d'altération.	En cas d'accès à la borne de recharge par un utilisateur malveillant qui altérerait son contenu, des dysfonctionnements ou d'éventuels dommages risqueraient de survenir.	Il est donc impératif de procéder à une inspection régulière de la borne de recharge afin de déceler toute trace d'altération (rayures, déchirures, arrachements...). Installez la borne de recharge dans un environnement contrôlé ou installez des caméras de sécurité.
Protocoles de communication	Modbus RTU, DHCP, DNS et SSDP présentent des failles de sécurité.	En cas d'accès au réseau par un utilisateur malveillant, celui-ci peut intercepter et écouter les communications.	Pour la transmission de données sur un réseau interne, il convient d'envisager une segmentation physique ou logique du réseau. Pour la transmission de données sur un réseau externe, considérez l'encapsulation des communications dans un tunnel chiffré, un wrapper TLS ou une solution similaire.
Compte utilisateur de maintenance	Les informations d'identification par défaut font souvent l'objet d'un accès non autorisé de la part d'utilisateurs malveillants.	Si la mise en service de la borne de recharge n'a pas eu lieu et le code PIN par défaut est resté inchangé, cela peut entraîner un accès non autorisé.	Changer en conséquence le code PIN par défaut par le biais de l'application de mise en service. Envisagez par ailleurs de renouveler régulièrement le code PIN.
	Les codes PIN d'un même compte utilisateur servent à différentes bornes de recharge.	Un utilisateur malveillant peut accéder à toutes les autres bornes de recharge configurées avec le même code PIN s'il connaît ce code.	Vous pouvez installer plusieurs bornes de recharge en configurant des codes PIN différents pour chacune d'entre elles.
Badges RFID	Il est possible de falsifier ou de dupliquer un badge.	Tout utilisateur malveillant qui met la main sur un badge RFID peut être en mesure de le reproduire et d'usurper l'identité d'un utilisateur légitime de la borne de recharge.	Il ne faut pas laisser les badges RFID sans surveillance. En cas de suspicion de duplication ou de falsification d'un badge, révoquer et renouveler les badges.

Conseils de sécurité

Recommandations pour la mise en service

Code PIN par défaut

La borne de recharge Schneider Charge Pro dispose d'un compte utilisateur par défaut pour la connexion initiale au produit à l'aide de l'application de mise en service lors de l'installation.

Le code PIN de ce compte est décrit dans la documentation utilisateur. Il est donc préférable de le changer par un nouveau code PIN au moyen de l'application de mise en service.

Il convient que le nouveau code PIN respecte les meilleures pratiques en matière de sécurité, notamment en utilisant un minimum de 8 chiffres et en évitant les schémas faciles à deviner (blocs de chiffres similaires ou incréments séquentiels de chiffres).

Sécurité de la communication OCPP

Il est recommandé de toujours utiliser WSS ou HTTPS pour sécuriser la communication lors de la configuration des bornes de recharge Schneider Charge Pro pour se connecter à un système de gestion à distance des bornes avec OCPP.

Les communications reposant sur le HTTP simple ou les sockets Web simples compromettent la sécurité et sont sujettes à des attaques de type « Man-In-The-Middle ».

Sécurité de SSDP

SSDP ne doit être activé que lorsque nécessaire.

Pour la sécurité du réseau, suivez ces bonnes pratiques lors de l'activation de SSDP :

Environnement réseau

- Limitez SSDP au réseau interne. Assurez-vous que le réseau est isolé d'internet pour empêcher toute exposition publique.

Bloquer l'accès externe

- Désactivez UPnP sur votre routeur pour bloquer les requêtes de découverte externes.
- Configurez des règles de pare-feu pour limiter l'accès au port SSDP (par défaut : UDP 1900) uniquement au trafic interne.

Recommandations de sécurité renforcée

- Pour une isolation plus stricte, utilisez des VLANs ou une segmentation réseau pour séparer les appareils avec SSDP activé.
- Examinez régulièrement la configuration du routeur et des équipements réseau pour vous assurer qu'aucune règle de redirection de port n'expose SSDP à internet.

Important : Le non-respect de ces mesures peut rendre les appareils vulnérables aux attaques externes ou aux analyses non autorisées. Une conformité stricte est requise.

Configuration des services

La plupart des services de la borne de recharge Schneider Charge Pro sont désactivés par défaut afin de réduire au minimum la surface d'attaque et l'exposition.

Il est par conséquent préférable de limiter l'activation de ces services à ceux qui sont strictement nécessaires. Les services non utilisés ne doivent pas être activés.

De même, lorsqu'un service n'est plus nécessaire ou utilisé, il est conseillé de le désactiver.

Conseils de sécurité pour le fonctionnement

Mise à jour du micrologiciel

La borne de recharge Schneider Charge Pro est dotée d'un micrologiciel nécessitant potentiellement la mise en place de correctifs de sécurité afin de maintenir un niveau de sécurité optimal.

Il est donc préférable de procéder à des vérifications régulières visant à garantir que le micrologiciel installé est le dernier disponible.

Les mises à jour du micrologiciel et les notes de mise à jour peuvent être téléchargées sur notre site web à l'adresse suivante https://www.se.com/fr/fr/download/.

Journal d'audit

Un journal d'audit est tenu par la borne de recharge Schneider Charge Pro permettant le suivi des événements liés à la sécurité, tels que les redémarrages, les mises à jour du micrologiciel et les tentatives de connexion non valides.

Il est ainsi conseillé de procéder régulièrement à une vérification des journaux d'audit afin de détecter d'éventuels comportements inattendus ou incorrects.

Conseils de sécurité en cas de mise hors service

Réinitialisation aux paramètres d'usine

La borne de recharge Schneider Charge Pro est configurée avec des informations sensibles concernant l'utilisateur, telles que les identifiants de compte d'utilisateur, les mots de passe, les identifiants de badge RFID et l'historique des opérations de charge.

Il est nécessaire, lors de la mise au rebut du produit, d'effectuer une réinitialisation aux paramètres d'usine du produit afin d'effacer toutes les informations sensibles ou confidentielles de l'utilisateur et de s'assurer qu'elles ne seront pas divulguées ou réutilisées.

Annexe A

Logiciels libres utilisés dans le Schneider Charge Pro

Le Schneider Charge Pro (« le produit ») intègre, entre autres, des Composants de Logiciels Libres (« OSS »), précisés ci-dessous, élaborés par des tiers et concédés sous une licence de logiciels libres. Ceux-ci bénéficient de la protection du droit d'auteur et d'autres formes de propriété intellectuelle. Votre droit d'utiliser les OSS est régi par les conditions de la licence OSS applicable.

Garantie relative à toute utilisation du logiciel libre :

La clause de non-responsabilité suivante vaut pour les composants GPL et LGPL par rapport aux détenteurs de droits :

« Les détenteurs des droits d'auteur distribuent les présents programmes animés par l'espoir qu'ils seront utiles, mais SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D'ADAPTATION À UN USAGE PARTICULIER ». Consultez la licence publique générale GNU ou la licence publique générale amoindrie GNU pour plus de détails.

Les autres composants à source ouverte sont soumis aux exclusions de responsabilité des détenteurs de droits, conformément à la licence correspondante.

Schneider Electric SE et toutes ses filiales (« Groupe Schneider Electric ») ne garantissent le logiciel libre intégré dans le produit, si celui-ci est mis en œuvre différemment de ce qui a été prévu par le Groupe Schneider Electric. Les licences énumérées ci-dessous définissent la garantie, le cas échéant, des détenteurs de droits des logiciels libres. Le groupe Schneider Electric ne garantit pas les défauts occasionnés par l'altération des logiciels libres ou de la configuration du produit. Tout recours en garantie à l'encontre du groupe Schneider Electric dans le cas où le logiciel libre contenu dans le Produit violerait les droits de propriété intellectuelle d'un tiers est exclu.

Le cas échéant, seule est fournie l'assistance technique aux logiciels non modifiés.

Autres utilisations du logiciel libre :

En respectant ces conditions de licence, vous aurez le droit d'utiliser les OSS de la manière prévue dans la licence concernée. Les conditions OSS font foi en cas de conflit entre d'autres conditions de licence de Schneider Electric applicables au produit et les conditions de licence OSS. Le logiciel libre est fourni sans redevance (c'est-à-dire que l'exercice des droits sous licence n'est pas soumis à redevance). Le logiciel libre ci-après fait partie de ce produit :

Nom du logiciel libre	Licence	Lien source	URL du texte de la licence
busybox	GPL-2.0	https://www.busybox.net/downlo ads/ busybox-1.36.1.tar.bz2	https://www.busybox.net/license.html
cgic	AFL-2.1 or GPL-2.0+ (library, tools), GPL-2.0+ (tools)	https://github.com/FastCGI-Archives/ fcgi2/archive/refs/tags/ 2.4.1.tar.gz	https://spdx.org/licenses/preview/OML. html
dbus	AFL-2.1 or GPL-2.0+ (library, tools), GPL-2.0+ (tools)	https://dbus.freedesktop.org/rele ases/dbus/dbus-1.14.10.tar.xz	https://spdx.org/licenses/AFL-2.1.html GNU General Public License version 2
e2fsprogs	GPL-2.0 (as a whole) LGPL-2.0 (lib/ext2fs and lib/e2p libraries) BSD-style license (lib/uuid library) MIT-like with advertising clause (libss and libet)	https://cdn.kernel.org/pub/linux/k ernel/people/tytso/e2fsprogs/v1. 47.0/ e2fsprogs-1.47.0.tar.xz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html https://www.gnu.org/licenses/old-licenses/lgpl-2.0.en.html
glibc	GPL-2.0+ (programs) LGPL-2.1+(as a whole) BSD-3-Clause MIT (library)	https://github.com/bminor/ glibc/a rchive/2.39-74-g198632a05f6c7b9ab67d3331d 8caace9ceabb685/glibc-2.39-74-g198632a05f6c7b9ab67d3331d 8caace9ceabb685.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html https://spdx.org/licenses/BSD-3-Clause.html
iptables	GPL-2.0	https://netfilter.org/projects/iptabl es/ files/iptables-1.8.10.tar.xz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
kmod	LGPL-2.1+ (library)	https://cdn.kernel.org/pub/linux/u tils/ kernel/kmod/kmod-31.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html
libatomic	GPL-3.0 with gcc exception	https://github.com/gcc-mirror/gcc/ tree/releases/gcc-12.3.0/libatomic	https://www.gnu.org/licenses/gpl-3.0.html
libnl	MIT with exceptions BSD-2 BSD-3 Apache 2.0 ZLIB CC-zero	https://github.com/warmcat/ libw ebsockets/archive/refs/tags/ v4.3.3.tar.gz	https://opensource.org/licenses/MIT https://opensource.org/license/bsd-2-clause/ https://opensource.org/license/bsd-3-clause/ https://www.apache.org/licenses/ LICENSE-2.0.html https://www.apache.org/licenses/ LICENSE-2.0.html https://creativecommons.org/pu blicdomain/zero/1.0/
libwebsockets	MIT with exceptions BSD-2 BSD-3 Apache 2.0 ZLIB CC-zero	https://github.com/warmcat/ libw ebsockets/archive/refs/tags/ v4.3.3.tar.gz	https://opensource.org/licenses/MIT https://opensource.org/license/bsd-2-clause/ https://opensource.org/license/bsd-3-clause/ https://www.apache.org/licenses/ LICENSE-2.0.html https://www.apache.org/licenses/ LICENSE-2.0.html https://creativecommons.org/ publicdomain/zero/1.0/
linux_kernel	GPL-2.0 WITH Linux-syscall-note and GCC exception GFDL 1.1 GFDL 1.2 GPL 1.0 ISCX Linux-OpenIB X11 zlib Apache-2.0 CDDL 1.0 cc-by-4.0 mpl 1.1	https://www.st.com/content/ccc/ resource/technical/software/firmware/ group1/87/b0/dd/40/30/7e/43/be/ stm32mp1dev/files/SOURCES-stm32mp1-openstlinux-5.15-yocto-kirkstone-mp1-v22.11.23. tar.gz/jcr:content/translations/ en.SOURCES-stm32mp1-openstlinux-5.15-yocto-kirkstone-mp1-v22.11.23.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html

tdb	LGPL-2.0	https://cdn.kernel.org/pub/linux/kernel/people/tytso/e2fsprogs/v1.47.0/e2fsprogs-1.47.0.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.0.en.html
u-boot	GPL-2.0+	https://github.com/u-boot/u-boot/archive/refs/tags/v2021.10.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
util-linux	GPL-2.0 GPL-2.0+ GPL-3.0+ LGPL-2.1+ (libblkid, libfdisk, libmount) BSD-2-Clause BSD-3-Clause (libuuid) BSD-4-Clause (xxhash) ISC (rfkill)	https://cdn.kernel.org/pub/linux/utils/util-linux/v2.39/util-linux-2.39.3.tar.gz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html https://opensource.org/license/BSD-3-clause
wireless-tools	GPL-2.0	https://hewlettpackard.github.io/wireless-tools/wireless_tools.30.pre9.tar.gz	https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html
zeromq	MPL v2	https://github.com/zeromq/libzmq/archive/refs/tags/v4.3.5.tar.gz	https://www.gnu.org/licenses/gpl-3.0.en.html https://www.gnu.org/licenses/lgpl-3.0.en.html https://www.mozilla.org/en-US/MPL/2.0
libxcrypt	LGPL-2.1+	https://github.com/besser82/libxcrypt/releases/download/v4.4.36/libxcrypt-4.4.36.tar.xz	https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
mmc-utils	GPL-2.0	https://git.kernel.org/pub/scm/utils/mmc/mmc-utils.git	https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

En cas de licence d’un logiciel libre (OSS) figurant dans le présent produit sous la licence générale publique GNU (GPL), Licence publique générale limitée GNU (LGPL), la licence publique Mozilla (MPL) ou toute autre licence d’OSS requérant la mise à disposition du code source, vous pouvez télécharger le code source du logiciel libre (OSS) en question en cliquant sur le lien susmentionné.

Schneider Electric Industries SAS

35, rue Joseph Monier
CS 30323
F - 92500 Rueil Malmaison Cedex

www.se.com

Étant donné la nature changeante des normes, des spécifications et de la conception, nous vous invitons à demander confirmation des renseignements figurant dans la présente publication.

© 2024 – 2025 Schneider Electric. Tous les droits sont réservés.

BRU5883000-02_FR