Recommandations relatives à la configuration sécurisée des produits Eaton

Powering Business Worldwide

Documentation pour déployer et configurer en toute sécurité les produits Eaton

La cybersécurité a été un facteur déterminant lors de la conception de la solution Eaton Green Motion AC Home. Ce produit propose plusieurs fonctionnalités pour pallier les risques liés à la cybersécurité. Ces recommandations relatives à la cybersécurité fournissent des informations qui aideront les utilisateurs à déployer et à gérer le produit de manière à minimiser les risques dans ce domaine. Ces recommandations de cybersécurité ne constituent pas un guide exhaustif de cybersécurité, mais viennent plutôt compléter les programmes de cybersécurité existants des clients.

Eaton s'efforce de minimiser les risques de cybersécurité dans ses produits et de développer des meilleures pratiques de cybersécurité dans ses produits et solutions pour les rendre plus sûrs, fiables et compétitifs pour les clients.

Vous trouverez de plus amples informations sur les meilleures pratiques et recommandations générales de cybersécurité dans les livres blancs suivants :

La cybersécurité pour les réseaux de distribution électrique (WP152002EN) :

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Liste de contrôle des meilleures pratiques de cybersécurité (WP910003EN) :

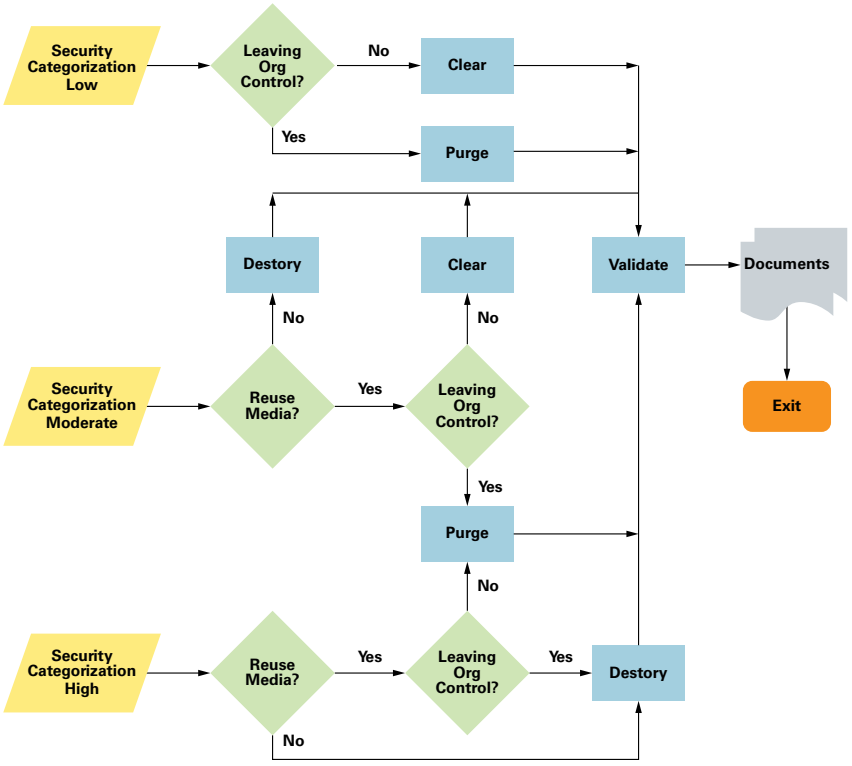
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

Meilleures pratiques en matière de cybersécurité pour les véhicules modernes - NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Catégorie	Description
Utilisation prévue et contexte de déploiement	Ce produit doit être utilisé pour charger les véhicules électriques des utilisateurs privés à domicile. Il est installé sur le site du client et peut être utilisé comme suit : 1. Mode hors ligne (pas de connexion à Internet) 2. Mode en ligne (connecté à Internet/au back-end) Pour plus d'informations sur l'utilisation et l'installation sécurisées du produit, consultez le lien suivant : www.eaton.com/greenmotionhome
Gestion des ressources	Pour une gestion efficace de la cybersécurité, le suivi des ressources logicielles et matérielles de votre environnement est un prérequis. Eaton vous recommande de tenir un inventaire des ressources identifiant de manière unique chaque composant important. Pour faciliter cela, **Eaton Green Motion AC Home** prend en charge les informations d'identification suivantes : Numéro de catalogue du produit, numéro de série (disponible sur le produit), détails du point d'accès usine, ID unique du dispositif (dépliants fournis avec le produit, à conserver en sécurité pour les besoins futurs). Reportez-vous au manuel d'installation pour plus d'informations.
Sécurité physique	Une personne malveillante disposant d'un accès physique non autorisé peut provoquer de graves interruptions du système/dispositif. Dans de tels cas, la sécurité physique est une ligne de défense importante. **Eaton Green Motion AC Home** est conçu pour être déployé et utilisé dans un emplacement physiquement sécurisé. Vous trouverez ci-dessous des exemples de meilleures pratiques recommandées par Eaton pour sécuriser physiquement votre système/dispositif : • Protégez l'installation et les salles ou armoires d'équipements à l'aide de mécanismes de contrôle d'accès (verrous, lecteurs de cartes d'entrée, protections, sas, vidéosurveillance, etc., selon le cas). • L'accès physique aux lignes de télécommunications et au câblage du réseau doit être restreint pour garantir la protection contre les tentatives d'interception ou de sabotage des communications. Une meilleure pratique consiste à utiliser des conduits métalliques pour le câblage du réseau entre les différentes armoires d'équipements. • **Eaton Green Motion AC Home** prend en charge les ports d'accès physiques suivants : Ethernet, port série, port USB. L'accès à ces ports doit être restreint pour les utilisateurs non autorisés. • Ne connectez pas de supports amovibles (par exemple, des périphériques USB, des cartes SD, etc.)
Gestion de comptes	L'accès logique au dispositif/système doit être limité aux utilisateurs légitimes. Il peut s'avérer nécessaire de mettre en œuvre certaines des meilleures pratiques suivantes, qui ne doivent se voir attribuer que les privilèges nécessaires à l'accomplissement de leurs rôles/fonctions professionnelles. Il peut être nécessaire de mettre en œuvre certaines des meilleures pratiques suivantes : • Assurez-vous que les informations d'identification par défaut sont modifiées lors de la première connexion. La solution Eaton Green Motion AC Home ne doit pas être déployée dans des environnements de production avec les informations d'identification par défaut, car celles-ci sont publiquement connues. • Pas de partage de compte : chaque utilisateur doit se voir attribuer un compte unique plutôt que de partager des comptes et des mots de passe. Les fonctionnalités de surveillance/d'enregistrement de la sécurité du produit sont personnalisées pour chaque utilisateur disposant d'un compte unique. Le fait d'autoriser les utilisateurs à partager des informations d'identification compromet la sécurité. • Assurez-vous que les exigences en termes de longueur, de complexité et d'expiration des mots de passe sont correctement définies, et plus particulièrement pour tous les comptes d'administration (par exemple, 10 caractères minimum, combinaisons de majuscules, minuscules et caractères spéciaux, expiration tous les 90 jours ou autres, conformément aux politiques de votre entreprise). - Politiques de mot de passe et de compte prises en charge : - Hotspot, 16 caractères, caractères A-F, 0-9 et spéciaux Uniquement accessibles dans la plage Wi-Fi, délai de 30 minutes, délai de verrouillage du système L'utilisateur doit définir un mot de passe complexe sur son routeur domestique Les comptes série et SSH sont destinés à être utilisés uniquement par le support technique Eaton à des fins de débogage/dépannage.

Catégorie	Description
Synchronisation du temps	De nombreuses opérations des réseaux électriques et informatiques dépendent fortement d'informations temporelles précises. Assurez-vous que l'horloge du système est synchronisée avec une source de temps fiable (via une configuration manuelle, NTP, SNTP ou IEEE 1588). En mode en ligne, la synchronisation de l'heure se produit automatiquement une fois que le terminal a accès à la notification de démarrage OCPP et à Heartbeat. En mode hors ligne, la synchronisation de l'heure se produit lorsque vous êtes connecté à l'application mobile. Tous les horodatages se font sur le fuseau horaire UTC.
Sécurité du réseau	**Eaton Green Motion AC Home** prend en charge la communication réseau avec d'autres dispositifs dans l'environnement. Cette fonction peut présenter des risques de sécurité si elle n'est pas correctement configurée. Vous trouverez ci-dessous des meilleures pratiques recommandées par Eaton pour sécuriser le réseau. Des informations supplémentaires sur diverses stratégies de protection du réseau sont disponibles dans le document La cybersécurité pour les réseaux de distribution électrique [R1] d'Eaton. Eaton recommande de segmenter les réseaux en groupes logiques, en bloquant le trafic entre les segments s'il n'est pas explicitement autorisé, et en limitant la communication aux chemins entre hôtes (à l'aide d'ACL de routeur et de règles de pare-feu par exemple). Ceci permet de protéger les informations sensibles et les services critiques, et de disposer de protections supplémentaires en cas de violation du périmètre du réseau. Pour un meilleur contrôle de la sécurité, un réseau de systèmes de commande industriel public doit, au minimum, être segmenté en une architecture à trois niveaux (tel que recommandé par la norme NIST SP 800-82[R3]). Protection des communications : **Eaton Green Motion AC Home** assure le cryptage de ses communications réseau. Ce cryptage est activé par défaut. Eaton recommande de n'ouvrir que les ports nécessaires pour les opérations et de protéger les communications réseau à l'aide de systèmes de protection du réseau comme des pare-feu et des systèmes de détection/prévention des intrusions. En mode en ligne, le chargeur se connecte au back-end à l'aide du protocole OCPP. En mode hors ligne, le chargeur se connecte à l'application mobile via le Wi-Fi.
Accès à distance	L'accès à distance aux dispositifs/systèmes constitue un autre point d'entrée sur le réseau. Une gestion et une validation rigoureuses d'un tel point d'accès sont essentielles pour pouvoir garder le contrôle sur la sécurité ICS globale. • Les capacités d'accès à distance sont fournies par le protocole sécurisé OCPP sur TLS 1.2. • L'appareil envoie les activités consignées dans les journaux système au back-end via le protocole OCPP. • Les mises à jour du firmware sont envoyées aux dispositifs depuis le back-end via OCPP si le périphérique est en ligne. • Pour plus d'informations, consultez les meilleures pratiques d'Eaton en matière de cybersécurité [R2]
Enregistrement et gestion des événements	• Les statistiques de charge sont disponibles sur l'application mobile pour que l'utilisateur puisse les consulter. • Passez régulièrement les journaux en revue. • Les enregistrements sont disponibles en ligne via le système Charging Network Manager d'Eaton (back-end). Pour plus d'informations, consultez la documentation technique du produit ou contactez l'équipe d'assistance locale.
Défenses contre les logiciels malveillants	Eaton recommande de déployer les défenses appropriées contre les logiciels malveillants, afin de protéger le produit ou les plateformes utilisées pour exécuter le produit Eaton.

Catégorie	Description
Maintenance en toute sécurité	L'appareil inclut une connexion locale SSH pour permettre à un ingénieur de maintenance de dépanner les fonctionnalités de l'appareil, avec l'aide de l'administrateur du site. Le port SSH est désactivé par défaut. Cette connexion est réservée aux ingénieurs de maintenance. Le client n'est pas censé utiliser cette fonctionnalité. **Remarque :** l'activation du port TCP 22 est proposée à des fins de diagnostic uniquement et ne doit pas être activée. **Meilleures pratiques** Mettez le firmware du dispositif à jour avant de mettre ce dernier en production. Appliquez ensuite les mises à jour du firmware et les correctifs logiciels régulièrement. Eaton publie des correctifs et des mises à jour pour ses produits afin de les protéger contre les vulnérabilités détectées. Les mises à jour du firmware doivent être gérées et installées exclusivement via le système Charging Network Manager d'Eaton, ce qui garantit que vous utilisez des fichiers de firmware fiables. • Pour les bornes de recharge en mode en ligne (connectées à Internet), le chargeur VE se met à jour automatiquement lorsqu'une mise à jour est disponible. • Pour les bornes de recharge en mode hors ligne (non connectées à Internet), l'application mobile vous informe de la disponibilité d'une mise à jour et installe cette dernière. Le chargeur VE ne sera pas disponible pendant le téléchargement et la mise à niveau du firmware de l'appareil.
Mise hors service ou réinitialisation	Avant de mettre au rebut un dispositif contenant des données, une meilleure pratique consiste à supprimer ces dernières. Cela inclut les informations sensibles telles que les informations d'identification, les journaux, les informations RFID, etc. La mémoire flash peut être effacée à l'aide de la fonction de réinitialisation des paramètres d'usine. Reportez-vous au manuel d'installation pour plus d'informations.  **Figure 1 :** Flux de décision relatif au nettoyage et à la destruction * Figure et données de la norme NIST SP800-88 La station de recharge sera recyclée conformément à la procédure ISO9001. **Mémoire Flash intégrée sur les cartes et les dispositifs** Eaton recommande les méthodes de mise au rebut suivantes pour les cartes mères, les cartes périphériques comme les adaptateurs réseau ou tout autre adaptateur comprenant une mémoire flash non volatile. **Effacer :** Réinitialisez l'état sur les paramètres d'usine d'origine en appuyant sur le bouton de réinitialisation et en le maintenant enfoncé pendant au moins 5 secondes. Reportez-vous à la documentation technique pour plus de détails. **Supprimer :** La mémoire flash ne peut pas être facilement identifiée et retirée de la carte. Pour cette raison, Eaton recommande de détruire la carte informatique dans son intégralité. **Détruire :** Broyez, désintégrez, pulvérisez ou incinérez en brûlant le dispositif dans un incinérateur agréé.

Remarques

Références

[R1] La cybersécurité pour les réseaux de distribution électrique (WP152002EN) :
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Liste de contrôle des meilleures pratiques de cybersécurité (WP910003EN) :
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rév. 2, Guide de la sécurité des systèmes de contrôle industriel (ICS), mai 2015 :
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) « Guidelines on Firewalls and Firewall Policy », Publication spéciale 800-41 du NIST, octobre 2009 :
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, « Guidelines for Media Sanitization », septembre 2006 :
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] Meilleures pratiques en matière de cybersécurité pour les véhicules modernes - NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[R8] Caractérisation des menaces de sécurité potentielles pour les automobiles modernes - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Modélisation de la menace pour l'analyse de la sécurité automobile
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Eaton Industries France
Place de la Gare 2
1345 Le Lieu, Suisse

Publication N° MZ191002FR
Octobre 2022

Suivez-nous sur les réseaux sociaux pour connaître toutes les dernières informations sur les produits et le support.