Panorama des menaces sur la cybersécurité industrielle

Panorama des menaces sur la cybersécurité industrielle

Le nombre de vulnérabilités dans les composants de supervision industrielle ne cesse d'augmenter.
Vu l'augmentation de l'attention portée à la sécurité de la supervision industrielle au fil des dernières années, de plus en plus d'informations sur les vulnérabilités qui touchent ces systèmes sont publiées. Toutefois, ces vulnérabilités peuvent très bien avoir été présentes dans ces produits pendant des années avant d'être dévoilées. C'est un total de 189 vulnérabilités dans des composants de supervision industrielle qui a été publié en 2015 et la majorité d'entre elles était critique (49 %) ou de gravité moyenne (42 %).

Vulnérabilités de supervision industrielle par année.

Les vulnérabilités peuvent être exploitées.
Il existait des codes d'exploitation pour 26 des vulnérabilités publiées en 2015. De plus, pour bon nombre de vulnérabilités (comme les identifiants codés en dur), un code d'exploitation n'est absolument pas requis pour obtenir un accès non autorisé au système vulnérable. Qui plus est, nos projets d'évaluation de la sécurité de la supervision industrielle montrent que les propriétaires de solutions de supervision industrielle considèrent souvent celles-ci comme une « boîte noire », ce qui signifie que les identifiants par défaut des composants de supervision industrielle restent souvent inchangés et peuvent être utilisés pour obtenir un contrôle à distance du système. Le projet SCADAPASS de l'équipe SCADA Strangelove fournit une représentation des identifiants par défaut de supervision industrielle connus. Le projet dispose actuellement d'informations sur 134 composants de supervision industrielle de 50 éditeurs.

Vulnérabilités dans la supervision industrielle en 2015 par niveau de risque (CVSS v.2 et CVSS v.3)

Les vulnérabilités dans les composants de supervision industrielle sont très diverses.
De nouvelles vulnérabilités ont été détectées en 2015 dans les composants de supervision industrielle de différents éditeurs (55 fabricants différents) et types (interface homme-machine, dispositifs électriques, SCADA, périphériques de réseau industriel, automates programmables industriels, et bien d'autres). Le plus grand nombre de vulnérabilités a été détecté chez Siemens, Schneider Electric et Hospira Devices. Les vulnérabilités dans les composants de supervision industrielle sont de nature différente. Les types les plus répandus sont les débordements de tampon (9 % de l'ensemble des vulnérabilités détectées), utilisation des identifiants codés en dur (7 %) et le cross-site scripting (7 %).

Toutes les vulnérabilités découvertes en 2015 n'ont pas été éliminées.
Il existe des correctifs et de nouveaux micrologiciels pour 85 % des vulnérabilités publiées. Les 15 % restants n'ont pas été réparés ou n'ont été que partiellement réparés pour différentes raisons. La majorité des vulnérabilités qui n'ont pas été éliminées (14 sur 19) présente un risque élevé. Ces vulnérabilités sans correctif représentent un risque significatif pour les propriétaires des systèmes concernés, surtout pour ceux chez qui les systèmes de supervision industrielle vulnérables sont exposés à Internet en raison d'une gestion inadéquate de la configuration réseau. A titre d'exemple, citons 11 904 interfaces SMA Solar Sunny WebBox accessibles à distance qui pourraient être compromises via les mots de passe codés en dur. Bien que ce nombre a considérablement diminué pour Sunny WebBox depuis 2014 (à l'époque, plus de 80 000 composants disponibles avaient été identifiés), il est toujours élevé et le problème des identifiants codés en dur (publié en 2015) qui n'a pas été résolu expose ces systèmes à un risque bien plus élevé qu'on ne le pensait jusqu'à présent.

Application de correctif dans les systèmes de supervision industrielle

De nombreux composants de supervision industrielle sont disponibles via Internet.
220 668 composants de supervision industrielle ont été découverts via le moteur de recherche Shodan. Ils sont installés sur 188 019 hôtes dans 170 pays. La majorité des hôtes accessibles à distance et dotés de composants de supervision industrielle est située aux Etats-Unis (30,5 %) et en Europe. Parmi les pays européens, l'Allemagne arrive en première position (13,9 %), suivie de l'Espagne (5,9 %). Les systèmes disponibles proviennent de 133 éditeurs différents. Les plus répandus sont Tridium (11,1 %), Sierra Wireless (8,1 %) et Beck IPC (6,7 %).

Top 20 des pays par disponibilité de composants de supervision industrielle

Les composants de supervision industrielle accessibles à distance utilisent souvent des protocoles qui ne sont pas sécurisés.
Il existe un certain nombre de protocoles, ouverts et non sécurisés par nature, comme HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 et de nombreux autres. Ils sont utilisés sur 172 338 hôtes différents, soit 91,6 % de l'ensemble des périphériques de supervision industrielle accessibles depuis l'extérieur trouvés. Les attaquants disposent ainsi de méthodes complémentaires pour compromettre les dispositifs via des attaques de type « homme au milieu ».

Top 15 des protocoles des composants de supervision industrielle accessibles depuis l'extérieur

De nombreux composants de supervision industrielle vulnérables sont accessibles depuis l'extérieur.
Nous avons répertorié 13 033 vulnérabilités sur 11 882 hôtes (soit 6,3 % de l'ensemble des hôtes dotés de composants accessibles depuis l'extérieur). Les vulnérabilités les plus répandues sont Sunny WebBox Hard-Coded Credentials (CVE-2015-3964) et les vulnérabilités critiques CVE-2015-1015 et CVE-2015-0087 dans Omron CJ2M PLC. Si nous combinons ces résultats aux statistiques d'utilisation de protocoles non sécurisés, nous pouvons estimer le nombre total d'hôtes de supervision industrielle vulnérables à 172 982 (92 %).

Top 5 des vulnérabilités dans les composants de supervision industrielle

Plusieurs secteurs sont touchés.
Nous avons découvert au moins 17 042 composants de supervision industrielle sur 13 698 hôtes différents dans 104 pays et probablement présents dans de grandes entreprises. La disponibilité de ces composants sur Internet est probablement associée à des risques élevés. Parmi les propriétaires, nous avons pu identifier 1 433 grandes entreprises, dont certaines appartenant aux secteurs d'activité suivants : électricité, aérospatial, transport (y compris les aéroports), pétrole et gaz, métallurgie, chimie, agriculture, automobile, distribution d'eau, de gaz et d'électricité, agroalimentaire, construction, réservoirs de stockage de liquide, villes intelligentes et éditeurs de solution de supervision industrielle. Des institutions académiques et de recherche, des institutions gouvernementales (y compris la police), des centres médicaux, des organisations financières, des complexes hôteliers, des musées, des bibliothèques, des églises et de nombreuses petites entreprises figurent également parmi les propriétaires de systèmes de supervision industrielle accessibles à distance identifiés. Le nombre d'hôtes de supervision industrielle vulnérables accessibles depuis l'extérieur qui appartiennent probablement à de grandes organisations s'élève à 12 483 (91,1 %) où 453 hôtes (3,3 %), dont des hôtes actifs dans le secteur de l'énergie, des transports, du gaz, de l'ingénierie et de l'industrie et de l'agroalimentaire, contenaient des vulnérabilités critiques.

Disponibilité des systèmes de supervision industrielle par éditeur

Les résultats ci-dessus ne sont que la limite inférieure des estimations. Le nombre réel de composants de supervision industrielle accessibles associés à de gros risques pourrait être bien plus élevé.

Conclusion

En matière de protection, l'isolement des environnements critiques ne peut plus être considéré comme une mesure de contrôle de la sécurité suffisante pour la supervision industrielle. Les exigences des activités économiques au 21e siècle imposent souvent la nécessité d'intégrer la supervision industrielle à des systèmes et des réseaux externes. De plus, les capacités, les motivations et le nombre des auteurs de menaces qui se concentrent sur les systèmes de supervision industrielle augmentent. Depuis les disques durs ou les clés USB infectés jusqu'aux connexions non autorisées depuis des réseaux de supervision industrielle à Internet via des smartphones ou des modems en passant par les kits d'installation infectés obtenus auprès d'un éditeur ou le recrutement d'un initié, toutes ces méthodes sont à la disposition d'individus malintentionnés très qualifiés qui préparent des attaques contre des réseaux de supervision industrielle isolés physiquement et logiquement.
Les propriétaires de systèmes de supervision industrielle doivent être au courant des vulnérabilités et des menaces modernes et exploiter ces informations pour améliorer la sécurité de leur environnement de supervision industrielle. Ici, le soutien actif de l'éditeur joue un rôle crucial dans l'identification et l'élimination rapides des vulnérabilités du système de supervision industrielle ainsi que dans le partage de solutions temporaires qui permettent de protéger les systèmes jusqu'à la publication des correctifs.
Les caractéristiques des systèmes de supervision industrielle, à savoir que leur sécurité sur le plan informatique est étroitement liée à la sécurité physique, reçoivent souvent un traitement contraire au traitement exigé dans de telles conditions. Les petites et moyennes entreprises, ainsi que les particuliers, s'en remettent complètement aux éditeurs lorsqu'il s'agit de la sécurité de l'Internet des objets. Les consommateurs ne s'aventurent pas au-delà des étapes simples décrites dans les manuels. Ils disposent donc de dispositifs prêts à l'emploi et facilement accessibles, mais également vulnérables. Les grandes entreprises, de leur côté, mesurent bien les risques élevés associés à une configuration incorrecte de l'environnement de supervision industrielle. Toutefois, c'est pour cette même raison que les propriétaires des systèmes considèrent souvent les dispositifs de supervision industrielle comme des « boîtes noires » et ont peur de modifier l'environnement, y compris sous la forme d'améliorations de la cybersécurité.
Les résultats de cette recherche nous rappellent une fois de plus que le principe de la « Sécurité par l'obscurité » ne peut être invoqué pour atteindre une protection efficace contre les attaques modernes et que la sûreté des systèmes de supervision industrielle ne doit pas être négligée au profit de la sécurité car dans ce domaine, la sûreté et la sécurité sont étroitement liées.
Article original de Kaspersky

Réagissez à cet article

Original de l'article mis en page : Panorama des menaces sur la cybersécurité industrielle — Securelist