Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1367

(09/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité

Recommandation UIT-T X.1367

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1367

Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité

Résumé

La gestion des incidents de sécurité dans l'écosystème de l'Internet des objets (IoT) se heurte à deux problèmes. Le premier est l'incompatibilité des protocoles entre, d'une part, les réseaux informatiques utilisant le protocole de commande de transmission/le protocole Internet (TCP/IP) et, d'autre part, les dispositifs d'extrémité IoT. Le second concerne l'absence de compatibilité des codes d'erreur utilisés par les différents fabricants de dispositifs d'extrémité.

La Recommandation UIT-T X.1367 décrit un format normalisé de journal d'erreur qui peut être placé dans une charge utile de protocole, comme syslog (voir IETF RFC 5424), afin de convertir les informations relatives au journal d'erreur provenant d'un dispositif d'extrémité dans le format normalisé de journal d'erreur.

Cette Recommandation contient en outre un tableau normalisé de codes d'erreur, qui permet de résoudre le second problème. De cette manière, les incidents de sécurité qui se produisent dans les réseaux informatiques et les réseaux de dispositifs d'extrémité IoT peuvent être gérés dans leur intégralité.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1367	03-09-2020	17	11.1002/1000/14263

Mots clés

Dispositif d'extrémité, code d'erreur, format de journal d'erreur, intervention en cas d'incident, Internet des objets (IoT), opération de sécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1367

Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité

1 Domaine d'application

La présente Recommandation décrit un format normalisé de journal d'erreur pour l'Internet des objets qui peut être placé dans une charge utile de protocole, comme syslog [b-IETF RFC 5424], afin de convertir les informations relatives au journal d'erreur provenant d'un dispositif d'extrémité dans le format normalisé de journal d'erreur.

Elle contient en outre un tableau normalisé de codes d'erreur, afin de pallier le manque de compatibilité des codes d'erreur des dispositifs d'extrémité des différents fabricants. De cette manière, les incidents de sécurité qui se produisent dans les réseaux informatiques et les réseaux de dispositifs d'extrémité IoT peuvent être gérés dans leur intégralité.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 actionneur [b-UIT-T Y.4109]: dispositif qui accomplit des actions physiques en réaction à un signal d'entrée.

3.1.2 attaque [b-ISO 13491-1]: tentative d'obtention ou de modification d'informations sensibles ou d'un service sur un dispositif, par un adversaire qui n'y est pas autorisé.

3.1.3 authentification [b-UIT-T X.1277]: processus par lequel un utilisateur recourt à son authentificateur FIDO pour prouver à une partie utilisatrice qu'il est en possession d'une clé enregistrée.

3.1.4 autorisation [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.1.5 dispositif [b-UIT-T Y.4000]: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

3.1.6 Internet des objets (IoT, *Internet of things*) [b-UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

3.1.7 interface homme-machine (HMI, *human-machine interface*) [b-UIT-T H.320]: interface entre l'usager et le terminal consistant en une partie matérielle (transducteur électroacoustique, électro-optique, touches, etc.) et en une partie logicielle agissant sur l'état du terminal.

3.1.8 logiciel malveillant [b-ISO/CEI 27033-1]: logiciel conçu expressément pour endommager ou perturber un système, et nuire à la confidentialité, à l'intégrité et/ou à la disponibilité.

3.1.9 capteur [b-UIT-T Y.4105]: dispositif électronique qui détecte une condition physique ou un composé chimique et fournit un signal électronique proportionnel à la caractéristique observée.

3.1.10 objet [b-UIT-T Y.4000]: dans l'Internet des objets, objet du monde physique (objet physique) ou du monde de l'information (objet virtuel), pouvant être identifié et intégré dans des réseaux de communication.

3.1.11 vulnérabilité [b-ISO/CEI 27000]: faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 certification: attestation établie par une partie tierce concernant des produits, des processus, des systèmes ou des personnes.

NOTE – Définition établie à partir de celle figurant dans la norme [b-ISO/CEI 17000].

3.2.2 serveur de commande et de contrôle (C&C): serveur qui envoie des commandes à des ordinateurs (botnets), devenus des bots après avoir été infectés par un logiciel malveillant, et qui les contrôle.

3.2.3 chiffrement: transformation cryptographique de données produisant un cryptogramme.

NOTE – Cette définition est fondée sur celle de la Recommandation [b-UIT-T X.800].

3.2.4 dispositif d'extrémité de l'Internet des objets: dispositif terminal de l'écosystème IoT qui collecte des données du monde réel au moyen de capteurs ou qui agit sur le monde réel par l'intermédiaire d'actionneurs.

3.2.5 passerelle de l'Internet des objets (IoTGW, *Internet of things gateway*): dispositif assurant la connexion entre un réseau de dispositifs d'extrémité IoT et des réseaux informatiques accessibles à grande échelle, comme l'Internet.

3.2.6 microcontrôleur (MCU, *microcontroller unit*): microprocesseur embarqué qui comprend des unités arithmétiques, des unités de mémoire ainsi que des ports d'entrée/de sortie au sein d'un même circuit intégré.

3.2.7 équipe d'intervention en cas d'incident de sécurité (SIRT, *security incident response team*): équipe qui reçoit les rapports relatifs aux "incidents de sécurité", les étudie et intervient en conséquence.

3.2.8 centre des opérations de sécurité (SOC, *security operations centre*): division qui surveille l'état des ordinateurs et des réseaux dans l'organisation et qui intervient en cas de détection de signes d'activités malveillantes.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

C&C commande et contrôle

FW pare-feu (*firewall*)

HMI interface homme/machine (*human/machine interface*)

ID identifiant

IDS système de détection des intrusions (*intrusion detection system*)

IoT Internet des objets (*Internet of things*)

IoTGW passerelle de l'Internet des objets (*Internet of things gateway*)

IP protocole Internet (*Internet protocol*)

JSON notation des objets en JavaScript (*JavaScript object notation*)

LAN réseau local (*local area network*)

MCU microcontrôleur (*microcontroller unit*)

PC ordinateur personnel (*personal computer*)

SIRT équipe d'intervention en cas d'incident de sécurité (*security incident response team*)

SOC centre des opérations de sécurité (*security operations centre*)

TCP protocole de commande de transmission (*transmission control protocol*)

5 Conventions

Aucune.

6 Généralités

6.1 Gestion des erreurs actuelle dans un écosystème IoT

Dans le cadre de la gestion des erreurs dans l'IoT, si l'un des composants d'un système IoT tel qu'un capteur ou un actionneur est mis hors service, un code d'erreur est généré et sauvegardé dans un journal d'erreur. Si l'erreur ne survient que sporadiquement, aucune correction n'est nécessaire. Toutefois, si l'erreur persiste, le composant devrait être remplacé pour résoudre le problème.

La Figure 1 décrit un écosystème IoT classique, qui comporte des composants IoT tels que des microcontrôleurs (MCU) associés à des capteurs et des actionneurs, une passerelle de l'Internet des objets (IoTGW) ainsi qu'un nuage.

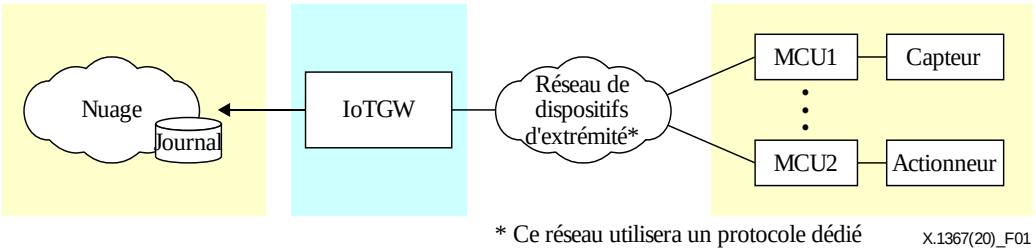

Figure 1 – Écosystème IoT classique

La communication entre la passerelle IoTGW et les microcontrôleurs MCU1 et MCU2 de la Figure 1 repose sur un protocole dédié (voir la note) propre au système. Le capteur (MCU1) et l'actionneur (MCU2) sont des exemples de dispositifs d'extrémité IoT. Dans ce cas, la passerelle IoTGW envoie une demande aux microcontrôleurs, qui lui répondent en lui transmettant une information journalisée. La passerelle IoTGW communique également avec le nuage (système dorsal).

NOTE – Le protocole dédié peut être l'un de ceux prévus pour les grands réseaux, tels que oneM2M [b-oneM2M] ou ECHONET Lite [b-ISO/CEI 14543-4-3], ou bien l'un de ceux prévus pour les petits réseaux, tels que SPI [b-SPI], I^2C [b-UM10204], Bluetooth [b-IEEE 802.15.1] ou Zigbee [b-IEEE 802.15.4], ou encore un protocole propriétaire conçu spécialement pour le système IoT en question.

Pour garantir une gestion appropriée de l'écosystème IoT, étant donné qu'il arrive que les dispositifs d'extrémité IoT subissent des pannes, l'écosystème IoT doit gérer les erreurs. Les systèmes en question traitent les journaux d'erreurs au moyen de codes d'erreur et réalisent les corrections appropriées. Par ailleurs, certains systèmes analysent les journaux d'erreurs enregistrés ainsi que les codes d'erreur, afin d'en extraire des informations statistiques pour améliorer le système, voire traiter les incidents de sécurité. Il est toutefois difficile d'unifier les journaux d'erreurs de tous les écosystèmes IoT et syslog [b-IETF RFC 5424].

6.2 Aperçu général

Pour intervenir efficacement lors des incidents, la fourniture de capacités adéquates pour le recueil et l'analyse des informations relatives aux journaux d'erreurs des composants de l'écosystème IoT constitue un élément clé. Cependant, les sujets de préoccupation suivants ont été relevés en ce qui concerne l'écosystème IoT:

1) Il existe une procédure normalisée qui comprend le processus relatif à la gestion des incidents au moyen de syslog [b-IETF RFC 5424] et qui permet de recueillir les informations journalisées des dispositifs de réseau. En revanche, il n'existe pas de telle procédure pour l'écosystème IoT.

2) Dans le cas de l'IoT, les informations relatives aux journaux d'erreurs ne peuvent pas être stockées dans un même composant de l'écosystème IoT, autrement dit, ces informations journalisées devraient être recueillies par le système dorsal (par exemple le nuage) ou par un système IoT d'extrémité (par exemple une passerelle IoTGW), selon la configuration de l'écosystème IoT.

3) Il est difficile d'effectuer une analyse de corrélation des informations relatives aux journaux d'erreurs entre différents composants IoT, car il n'existe pas de format normalisé de journal d'erreur.

4) En l'absence de méthode de gestion des informations relatives aux journaux d'erreurs, l'écosystème IoT ne sera pas en mesure de maintenir de manière efficace les services IoT qu'il fournit.

La présente Recommandation décrit une architecture de base pour un système IoT, permettant de recueillir les journaux d'erreurs IoT qui seront utilisés dans le cadre des opérations de gestion des incidents. Elle décrit des codes d'erreur normalisés ainsi qu'un format de journal d'erreur. En convertissant les codes d'erreur utilisés par chaque fabricant d'écosystème IoT en codes d'erreur normalisés, l'état de divers écosystèmes IoT pourrait être surveillé plus efficacement. En outre, lors du processus de conversion d'un code d'erreur en code d'erreur normalisé, la situation dans laquelle l'erreur a été générée est également enregistrée dans les journaux d'erreurs correspondants. De cette manière, les incidents de sécurité peuvent être traités au sein des écosystèmes IoT multiples. (Voir l'exemple dans l'Appendice I, § I.4, écosystèmes IoT multiples).

7 Format normalisé de journal d'erreur pour l'environnement IoT

En raison des faibles ressources informatiques dont ils disposent, les dispositifs d'extrémité IoT peuvent rencontrer des difficultés vis-à-vis de la mise en œuvre de nouvelles fonctions relatives à la gestion des journaux d'erreurs IoT. Cependant, une passerelle IoTGW dispose normalement de ressources informatiques plus adaptées à cette tâche. La passerelle IoTGW et les systèmes en nuage échangent régulièrement des demandes et des réponses; et ces communications comprennent des informations relatives aux journaux d'erreurs IoT. Par conséquent, dans le cadre de la présente Recommandation, une passerelle IoTGW doit générer des informations relatives aux journaux d'erreurs normalisées et les transmettre aux systèmes en nuage.

7.1 Structure de base du format de journal d'erreur

Le format d'un journal d'erreur IoT est celui décrit dans la Figure 2 au moyen de la notation des objets en JavaScript (JSON) avec des expressions régulières. Ce format peut être adapté en vue de son utilisation par syslog ou XML (voir la note). Des exemples de ce format sont décrits dans l'Appendice I.

NOTE – La présente Recommandation ne définit pas la longueur de la valeur de chaque attribut. L'expéditeur et le destinataire du journal d'erreur devront au préalable convenir d'un accord concernant la longueur de la valeur de chaque attribut.

```
{
   "Timestamp":
        "^([0-9]{4})-(1[0-2]|0[1-9])-(3[01]|0[1-9]|[12][0-9])T
          (2[0-3]|[01][0-9]):([0-5][0-9]):([0-5][0-9])(\.[0-9]{+})Z$",
   "Reporter": {},
   "Protocol": String,
   "Requester": {},
   "Responder": {},
   "Error Code": "/^[0-9A-F]^{+}$/",
   "Error Message": String,
   "Description": String | {},
}
```

Figure 2 – Éléments de l'enregistrement d'une erreur

Dans la plupart des cas, l'entité à l'origine de ce journal d'erreur est la passerelle IoTGW. Les attributs utilisés dans ce format sont définis au § 7.2.

7.2 Attributs de base

Les attributs suivants constituent des éléments d'information relatifs aux journaux d'erreurs.

a) Horodate *(Timestamp)*: une horodate (voir la note) est nécessaire pour la publication d'un journal d'erreur. Par exemple, pour le 20 septembre 2018, à 13 h 25 min 51 s, la valeur de l'horodate devrait être "2018-09-20T13:25:51.0Z."[b-ISO 8601-1].

NOTE – L'horodate est un attribut obligatoire, malgré la présence d'un autre champ "horodate" dans le protocole de transmission des journaux d'erreurs décrit dans la présente Recommandation, car la valeur de cet attribut change généralement entre le moment où le problème survient et le moment du transfert.

b) Rapporteur *(Reporter)*: composant IoT qui convertit le code d'erreur d'un dispositif en code d'erreur normalisé et qui l'envoie au nuage. La description détaillée est donnée dans la Figure 3.

```
"Reporter":{
    "IP Address":
        "(^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
              (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)
         |(^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$)"
}
```

Figure 3 – Éléments du rapporteur

1) Adresse IP *(IP Address)*: identifiant (ID) unique du rapporteur sur le réseau Ethernet.

c) Protocole *(Protocol)*: nom du protocole utilisé par la passerelle IoTGW et les dispositifs d'extrémité IoT.

d) Demandeur ou répondeur *(Requester (or Responder))*: composant IoT qui envoie une demande à un dispositif d'extrémité IoT ou composant IoT qui répond à une demande. La description détaillée est donnée dans la Figure 4.

```
"Requester(or Responder)": {
    "Unique ID": string,
    "Transmitted Code": "( [0-9A-F])^{+}}
```

Figure 4 – Éléments du demandeur et du répondeur

1) Identifiant unique *(Unique ID)* (facultatif): nombre ou code unique associé à chaque dispositif et défini par le protocole du réseau de dispositifs d'extrémité IoT.

2) Code transmis *(Transmitted code)* (facultatif): transmission du contenu des données. Il est exprimé sous forme hexadécimale.

3) Lorsqu'une erreur survient sans demandeur ou répondeur, l'attribut doit prendre la forme indiquée dans la Figure 5. C'est le cas notamment d'un capteur qui envoie périodiquement des données, sans demande en ce sens.

```
"Requester(or Responder)": {}
```

Figure 5 – Cas de l'absence de demandeur ou de répondeur

e) Code d'erreur, message d'erreur *(Error Code, Error Message)*: les codes d'erreur et les messages d'erreur sont indiqués dans l'Annexe A.

f) Description (facultatif): toute phrase, toute expression et tout sous-élément en notation JSON peuvent être indiqués, si une notification concernant l'état des dispositifs d'extrémité IoT ou leurs réseaux est nécessaire.

Le message d'erreur peut être omis si la bande passante est faible ou si l'espace de stockage est limité. La description peut être omise si aucun texte supplémentaire n'est nécessaire.

Annexe A

Codes d'erreur et messages d'erreur

(Cette annexe fait partie intégrante de la présente Recommandation.)

Les codes d'erreur et les messages d'erreur sont indiqués dans le Tableau A.1.

Tableau A.1 – Codes d'erreur et messages d'erreur

Code	Message	Description
	Aucune erreur (0x00-0x0F)	
0x00	Aucune erreur	Aucune erreur ne se produit.
	Communication (0x10-0x1F)	
0x10	Absence de réponse	Absence de réponse, bien que la demande en exige une (ou plusieurs).
0x11	Échec de la communication	Des problèmes ont entraîné un échec de la communication.
0x12	Liaison en panne	Une liaison d'interface de réseau est en panne.
0x1E	Raison détaillée	Préfixe indiquant une raison détaillée.
0x1F	Autres raisons relatives à la communication	Autres raisons relatives à la communication.
	Sécurité (0x20-0x2F)	
0x20	Échec de l'authentification	Des problèmes sont survenus lors de l'authentification.
0x21	Échec de la certification	Des problèmes sont survenus lors de la certification.
0x22	Échec du chiffrement	Des problèmes sont survenus lors du chiffrement.
0x23	Échec de l'autorisation	Des problèmes sont survenus lors de l'autorisation.
0x2E	Raison détaillée	Préfixe indiquant une raison détaillée.
0x2F	Autres raisons relatives à la sécurité	Autres raisons relatives à l'authentification, à la certification, au chiffrement ou à l'autorisation.
	Commande (0x30-0x3F)	
0x30	Commande non valable	La commande n'est pas définie ou n'est pas valable.
0x31	Argument non valable	L'argument ne se situe pas dans l'intervalle de validité ou n'est pas valable.
0x3E	Raison détaillée	Préfixe indiquant une raison détaillée.
0x3F	Autres raisons relatives à la commande	Autres raisons relatives à la commande.
	Dispositif (0x40-0x4F)	
0x40	Dispositif hors d'usage	Une partie du dispositif est irrémédiablement hors d'usage.
0x41	Panne du dispositif	Une partie du dispositif a subi une panne qu'il est possible de réparer.
0x42	Ressources insuffisantes	Manque de ressources de stockage, de mémoire ou de toutes autres ressources de calcul.
0x4E	Raison détaillée	Préfixe indiquant une raison détaillée.
0x4F	Autres raisons relatives au dispositif	Autres raisons relatives au dispositif.

Tableau A.1 – Codes d'erreur et messages d'erreur

Code	Message	Description
	Valeurs réservées en vue d'une extension future (0x50-0xDF)	
	Valeurs réservées pour les applications privées (0xE0-0xEF)	
	Autres (0xF0-0xFF)	
0xFF	Autres raisons	Autres raisons, à l'exception de celles mentionnées ci-dessus.

Appendice I

Exemples d'utilisation des journaux d'erreurs pour la gestion des incidents

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 L'auteur d'une attaque envoie une chaîne de caractères aléatoire à un dispositif d'extrémité par l'intermédiaire d'une passerelle IoTGW

La Figure I.1 illustre le cas où l'auteur d'une attaque envoie une chaîne de caractères aléatoire au microcontrôleur MCU1 ainsi que la réaction de ce dernier. L'en-tête de la chaîne de caractères aléatoire "01000001" désigne le dispositif N° 0001 et la fonction N° 0100. En d'autres termes, l'auteur de l'attaque vise la fonction N° 0100 du dispositif N° 0001. Le microcontrôleur MCU1 ne peut pas interpréter "3A459187F43CDDE5". Par conséquent, il envoie la réponse "000003FF" (commande inconnue) au dispositif N° 0000 (une passerelle IoTGW).

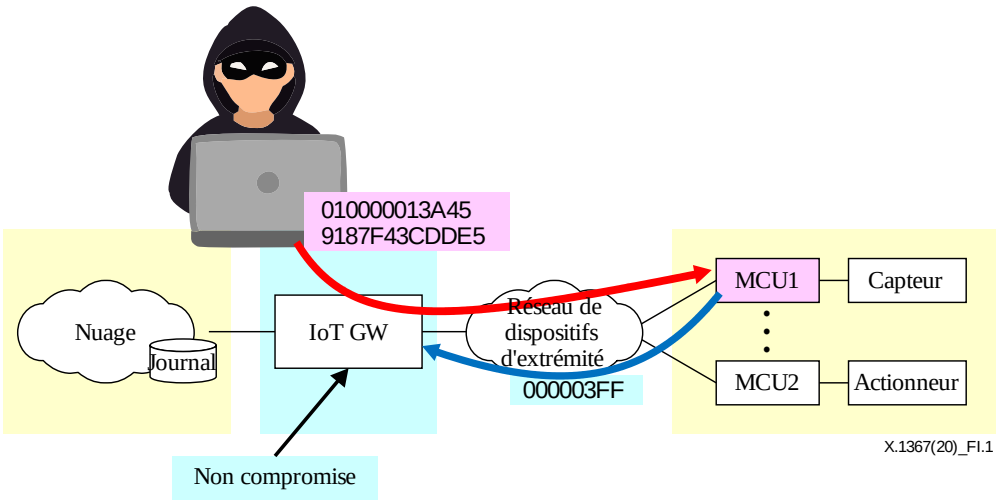

Figure I.1 – L'auteur d'une attaque envoie une chaîne de caractères aléatoire au microcontrôleur MCU1

Suite à la réception du code "000003FF" du microcontrôleur MCU1, la passerelle IoTGW établit le journal suivant et l'envoie à un serveur de journalisation dans le nuage. Voir la Figure I.2.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.2.11"},
    "Protocol": "ABC company protocol",
    "Requester": {
        "Unique ID": "0000",
        "Transmitted Code": "010000013A459187F43CdDE5"
    },
    "Responder": {
        "Unique ID": "0001",
        "Transmitted Code": "000003FF"
    },
    "Error Code": "30",
    "Error Message": "Invalid Command",
}
```

Figure I.2 – Journal d'erreur IoT en cas de demande inconnue (exemple)

I.2 L'auteur d'une attaque envoie une certification incorrecte à un dispositif d'extrémité par l'intermédiaire d'une passerelle IoTGW compromise

La Figure I.3 illustre le cas où l'auteur d'une attaque envoie une certification incorrecte au microcontrôleur MCU2 par l'intermédiaire d'une passerelle IoTGW compromise ainsi que la réaction du microcontrôleur. Le microcontrôleur MCU2 détecte que la certification n'est pas valable. Par conséquent, il envoie la réponse "00000010000c" (erreur lors de la vérification du certificat) au dispositif N° 0000 (une passerelle IoTGW). Cependant, la passerelle IoTGW est compromise. Elle n'enverra jamais de journal d'erreur au serveur de journalisation dans le nuage. Le système de détection des intrusions (IDS) envoie un journal d'erreur IoT à la place de la passerelle IoTGW.

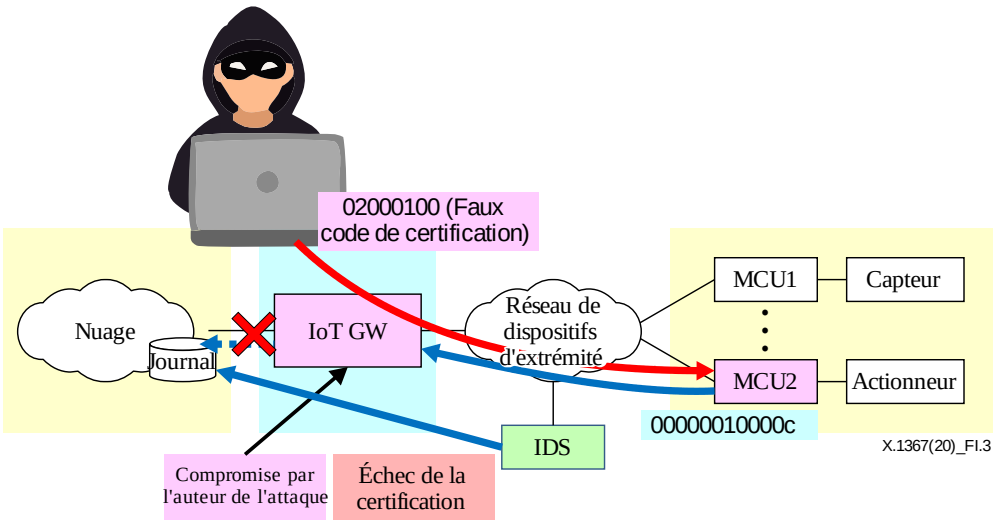

Figure I.3 – L'auteur d'une attaque envoie un faux code de certification

L'auteur de l'attaque envoie un faux code de certification au microcontrôleur MCU2, mais ce dernier ne peut pas le reconnaître. Par conséquent, il envoie la réponse "00000010000c" (erreur lors de la vérification du certificat). La passerelle IoTGW ignore le message de réponse du microcontrôleur MCU2, car elle a été compromise au préalable par l'auteur de l'attaque. Cependant, si le système est doté d'un système IDS, ce dernier établit le journal d'erreur IoT reproduit dans la Figure I.4 à la place de la passerelle IoTGW. Dans ce cas, le système IDS devient un rapporteur.

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.100.249"},
    "Protocol": "EEE Company's protocol",
    "Requester": {
        "Unique Name": "0000",
        "Transmitted Code": "02000100... (Faked certification codes)"
    },
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": "000000000010000c "
    },
    "Error Code": "21",
    "Error Message": "Certification Failed",
    "Description": {
        "Status": "This message was sent from IDS not IoTGW"
    },
}
```

Figure I.4 – Journal d'erreur IoT en cas d'erreur lors de la vérification du certificat (exemple)

I.3 L'auteur d'une attaque met physiquement hors d'usage un capteur qui envoie périodiquement des données, sans demande en ce sens

La Figure I.5 illustre le cas où l'auteur d'une attaque met physiquement hors d'usage le microcontrôleur MCU1, qui envoie périodiquement des données, sans demande en ce sens. Suite à cela, le microcontrôleur MCU1 ne peut plus envoyer de données. Dans ce cas, la passerelle IoTGW détecte une situation anormale concernant le microcontrôleur MCU1 et envoie le journal d'erreur IoT reproduit dans la Figure I.6.

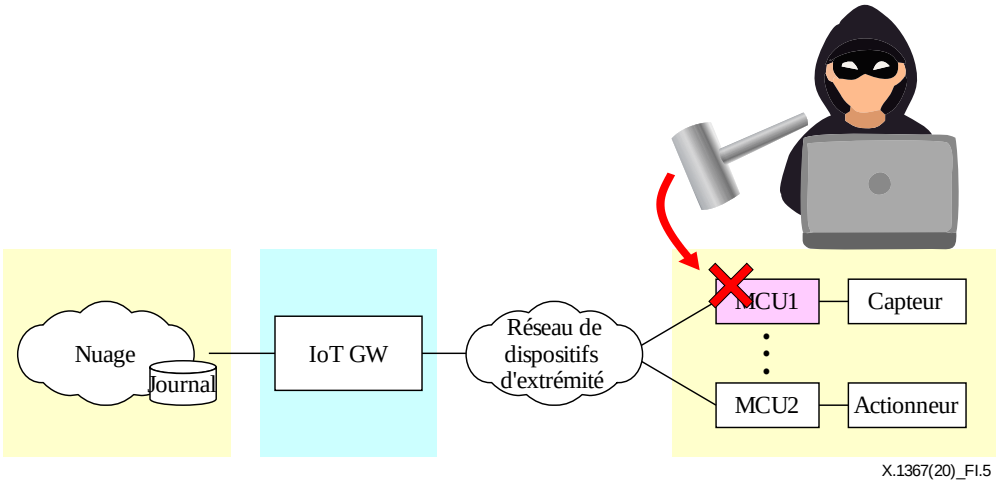

Figure I.5 – L'auteur d'une attaque met physiquement hors d'usage le microcontrôleur MCU1

```
{
    "Timestamp":"2018-08-28T09:34:55.0Z",
    "Reporter": { "IP Address": "192.168.10.254"},
    "Protocol": "ZZZ Company's protocol",
    "Requester": {},
    "Responder": {
        "Unique Name": "0002",
        "Transmitted Code": ""
    },
    "Error Code": "11",
    "Error Message": "Communication Failed",
    "Description": {
        "Responder stopped sending data."
    },
}
```

Figure I.6 – Journal d'erreur IoT envoyé en cas de perte de communication (exemple)

I.4 Utilisation des journaux IoT pour les interventions en cas d'incident

Une usine est dotée de trois écosystèmes IoT au sein d'un même réseau local (LAN), comme le montre la Figure I.7.

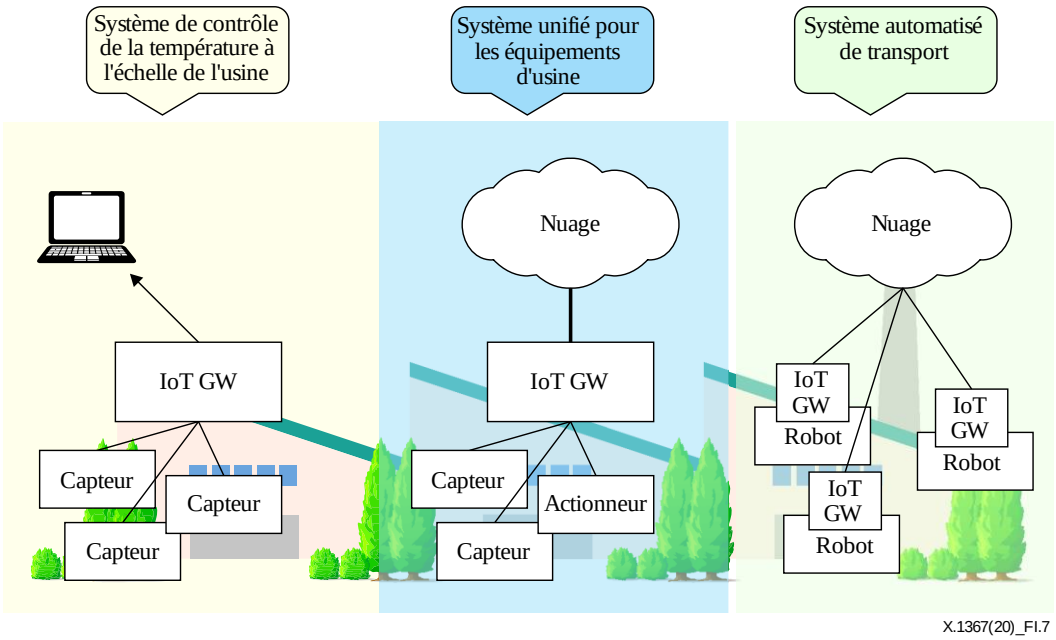

Figure I.7 – Écosystèmes IoT multiples dans une usine

Dans ce cas, l'auteur d'une attaque peut facilement prendre chaque dispositif comme cible, comme le montre la Figure I.8. En l'absence de journaux d'erreurs IoT, il est difficile pour l'équipe d'intervention en cas d'incident de sécurité (SIRT) d'identifier les traces laissées par l'auteur de l'attaque, car cette équipe ne peut pas unifier les journaux IoT non normalisés de chaque écosystème IoT.

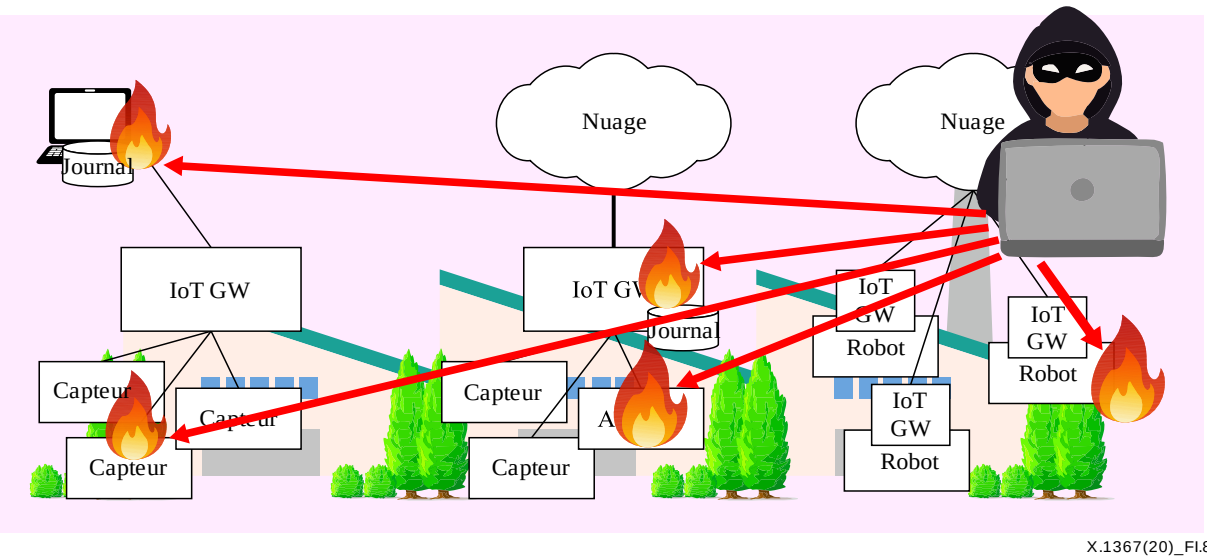

Figure I.8 – L'auteur d'une attaque prend tous les écosystèmes IoT pour cible en même temps

Si ces écosystèmes IoT utilisent le format de journal d'erreur IoT normalisé, l'équipe SIRT peut facilement unifier tous les journaux d'erreurs IoT, comme illustré dans la Figure I.9, de même qu'elle peut unifier les journaux syslog. Les traces laissées par l'auteur de l'attaque peuvent alors être identifiées.

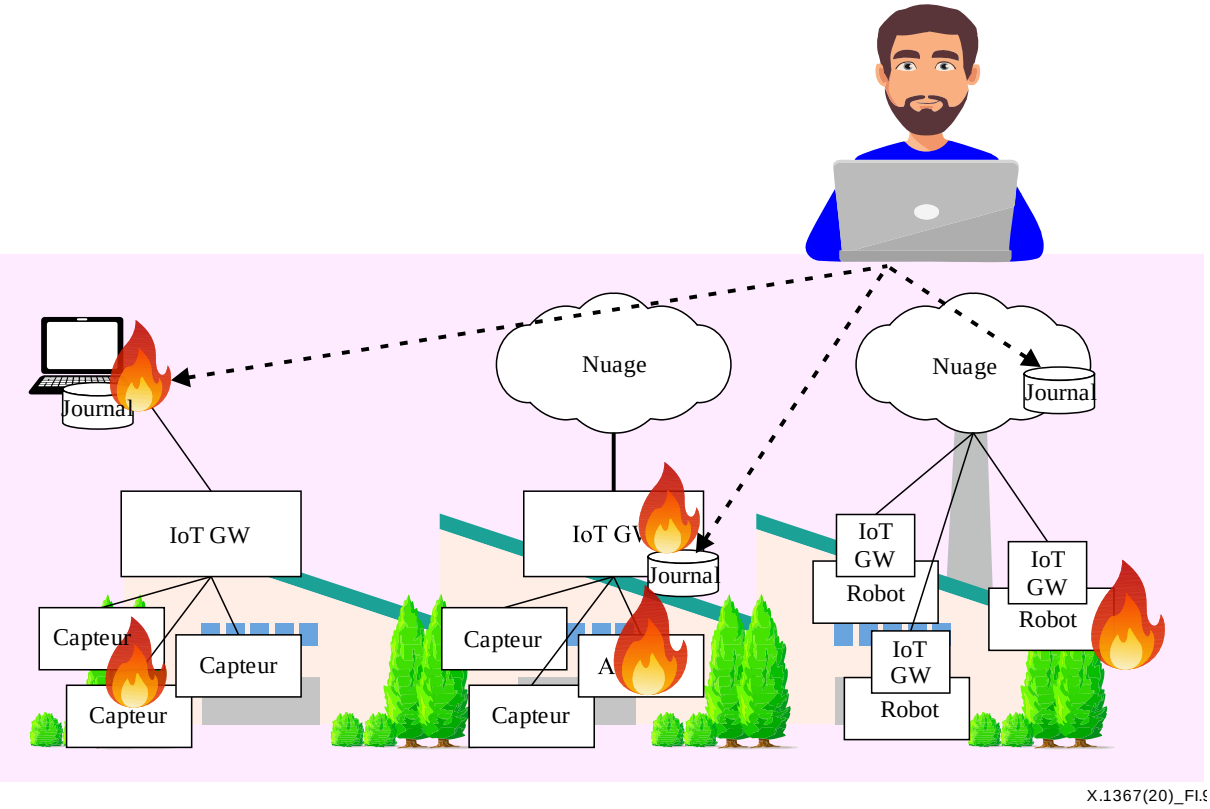

Figure I.9 – Unification et analyse de tous les journaux d'erreurs IoT

Appendice II

Intervention anticipée en cas d'incident de sécurité au moyen des journaux d'erreurs pour l'Internet des objets

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Les journaux d'erreurs IoT normalisés décrits dans la présente Recommandation peuvent être utilisés dans le cadre des interventions en cas d'incident de sécurité dans un écosystème IoT. La Figure II.1 illustre le flux correspondant à la détection d'un incident au moyen des journaux d'erreurs IoT.

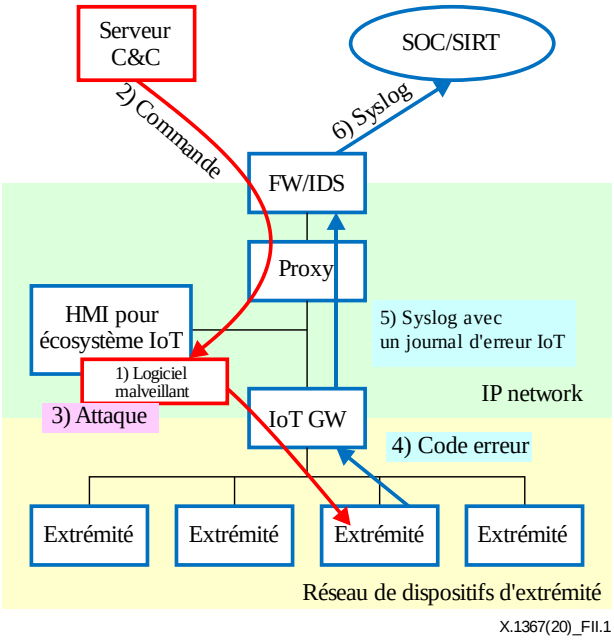

Figure II.1 – Détection d'un incident au moyen des journaux d'erreurs IoT

1) Un logiciel malveillant parvient, d'une manière ou d'une autre, à infecter une interface homme/machine (HMI), par exemple un ordinateur personnel de bureau (PC).

2) Le logiciel malveillant reçoit des commandes provenant du serveur de commande et de contrôle (C&C). Un pare-feu (FW), un système IDS ou un proxy peut enregistrer un journal contenant la communication entre le logiciel malveillant et le serveur C&C.

3) Le logiciel malveillant recherche une vulnérabilité du dispositif d'extrémité IoT. Le dispositif d'extrémité IoT envoie de nombreux codes d'erreur à la passerelle IoTGW, car le logiciel malveillant essaie de manière répétée d'envoyer des commandes avec différents paramètres. Dans la plupart des cas, les paramètres ne sont pas valables pour le dispositif d'extrémité IoT.

4) Pour chaque code d'erreur IoT envoyé, la passerelle IoTGW envoie un journal d'erreur IoT dans le format décrit dans la présente Recommandation au pare-feu ou au système IDS, en utilisant le protocole syslog.

5) Un proxy envoie aussi des journaux de communication en utilisant le protocole syslog au pare-feu ou au système IDS. Ce dernier envoie l'ensemble des journaux, y compris les journaux d'erreurs IoT, au moyen du protocole syslog, au centre des opérations de sécurité (SOC) ou à l'équipe SIRT.

Les analystes de la sécurité du centre SOC ou de l'équipe SIRT peuvent ne pas réagir face à un journal d'erreur IoT isolé, sans lien avec d'autres journaux d'erreurs IoT. En revanche, ils peuvent détecter une situation anormale si le centre SOC ou l'équipe SIRT reçoit, de manière continue, un grand nombre de journaux d'erreurs IoT, car cela pourrait être le signe que l'auteur d'une attaque recherche une vulnérabilité du système IoT.

La présente Recommandation permet aux analystes du centre SOC ou de l'équipe SIRT de détecter les attaques perpétrées sur les dispositifs d'extrémité IoT, car le centre SOC ou l'équipe SIRT reçoit des codes d'erreur IoT dans le format de journal d'erreur IoT normalisé. Ils pourront ainsi vérifier les autres journaux associés, y compris ceux contenant les communications entre le logiciel malveillant et le serveur C&C, et envoyer une notification à l'opérateur de l'usine, afin de déconnecter l'ordinateur personnel de bureau HMI concerné du réseau LAN ou de supprimer le logiciel malveillant de cet ordinateur.

Bibliographie

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.1277] Recommandation UIT-T X.1277 (2018), *Cadre d'authentification universelle.*

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets.*

[b-UIT-T Y.4105] Recommandation UIT-T Y.4105/Y.2221 (2010), *Prescriptions de prise en charge pour les applications et services de réseaux de capteurs ubiquitaires dans l'environnement des réseaux de prochaine génération.*

[b-UIT-T Y.4109] Recommandation UIT-T Y.4109/Y.2061 (2012), *Exigences relatives à la prise en charge des applications de communication orientée machine dans l'environnement des réseaux de prochaine génération.*

[b-ISO 8601-1] ISO 8601-1:2019, *Date et heure – Représentations pour l'échange d'information – Partie 1: Règles de base.*

[b-ISO 13491-1] ISO 13491-1:2016, *Services financiers – Dispositifs cryptographiques de sécurité (services aux particuliers) – Partie 1: Concepts, exigences et méthodes d'évaluation.*

[b-ISO/CEI 14543-4-3] ISO/ CEI 14543-4-3:2015, *Technologies de l'information – Architecture des systèmes électroniques domestiques (HES) – Partie 4-3: Interface de la couche d'application avec les couches inférieures de communication pour les dispositifs de contrôle de réseau améliorés de la classe HES 1.*

[b-ISO/CEI 17000] ISO/CEI 17000:2004, *Évaluation de la conformité – Vocabulaire et principes généraux.*

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts.*

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Technologies de l'information – Techniques de sécurité – Sélection, déploiement et opérations des systèmes de détection et prévention d'intrusion.*

[b-IEEE 802.15.1] IEEE 802.15.1-2005, *IEEE Standard for information technology – Local and metropolitan area networks – Specific requirements – Part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN).*

[b-IEEE 802.15.4] IEEE 802.15.4-2015, *IEEE Standard for low-rate wireless networks.*

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The syslog protocol*.

[b-oneM2M] oneM2M Partners (2017), Standards for M2M and Internet of things. Disponible à l'adresse [consultée le 12/02/2020]: http://www.onem2m.org/

[b-SPI] Motorola (2001), SPI block guide, V04.01. Disponible à l'adresse [consultée le 12/02/2020]: https://www.nxp.com/files-static/microcontrollers/doc/ref_manual/S12SPIV4.pdf

[b-UM10204] UM10204 (2014), *I^2C-bus specification and user manual*, Rév.6. Disponible à l'adresse [consultée le 12/02/2020]: https://www.nxp.com/docs/en/user-guide/UM10204.pdf

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021