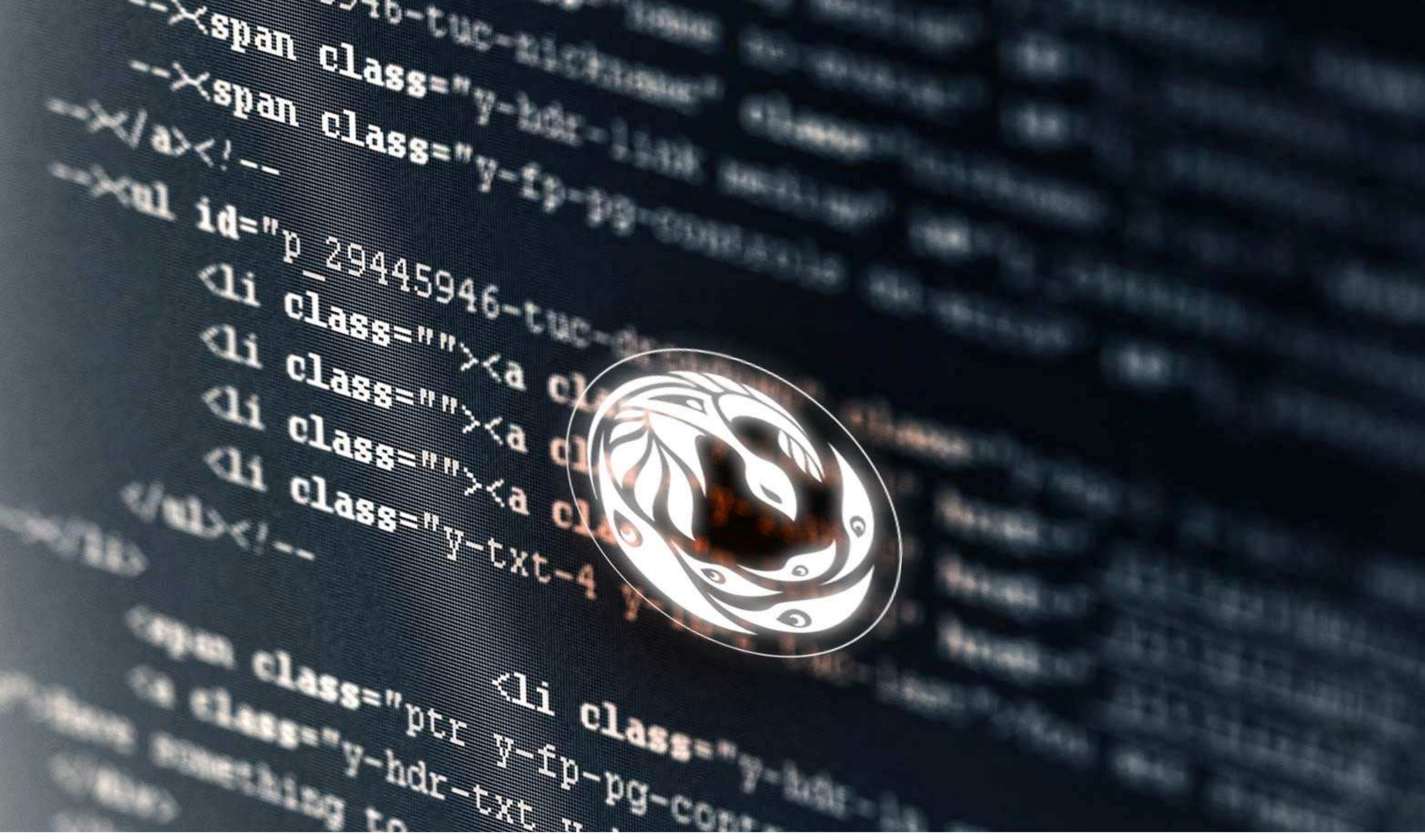


Gestion de vulnérabilités dans l’IoT : comment atteindre la cyber-résilience ?

Maxime ALAY-EDDINE
Cyberwatch SAS - http://www.cyberwatch.fr
v1.0 - 15/09/2016

Faisons connaissance !

- Maxime ALAY-EDDINE
- 25 ans, Consultant SSI & Développeur
- Président de Cyberwatch SAS
  - Tests d'intrusion
  - Logiciel de supervision des vulnérabilités / MCS
- Premiers pas dans la sécurité informatique à 12 ans

Centrale Nantes

SciencesPo

SAFRAN Sagem

Sport in town .com

Cyberwatch
cybersecurity as a service

La cyber-résilience ?

La cyber-résilience ?

Résilience :

« Caractéristique mécanique définissant la résistance aux chocs d'un matériau. »
(Larousse)

La cyber-résilience ?

Résilience :

« Caractéristique mécanique définissant la résistance aux chocs d'un matériau. »
(Larousse)

≠

Sécurité :

« Situation de quelqu'un qui se sent à l'abri du danger, qui est rassuré. »
(Larousse)

Sécurité dans l’IoT :

Comment limiter le risque que l’on porte atteinte
à la Disponibilité, à l’Intégrité, ou à la Confidentialité
de mon système embarqué ?

=> Résolution des risques <=

Résilience dans l’IoT :

En cas d’incident de sécurité,
comment limiter les dégâts sur un système embarqué ?

=> Résolution des incidents <=

Sécurité dans l'IoT :

Comment limiter le risque que l'on porte atteinte
à la Disponibilité, à l'Intégrité, ou à la Confidentialité
de mon système d'informations embarqué ?

=> Résolution des risques <=

Résilience dans l'IoT :

En cas d'incident de sécurité,
comment limiter les dégâts sur un système embarqué ?

=> Résolution des incidents <=

Quels sont les incidents les plus probables ?

Quels sont les incidents les plus probables ?

Exploitation d’une vulnérabilité connue.

Nous nous concentrerons dans la suite de cette présentation sur

la gestion des vulnérabilités et leur supervision dans le cadre de l'Internet des Objets.

Objectif :

Être résilient « by design »
face à de nouvelles vulnérabilités

Plan

1. Introduction
2. Cycle de vie d’une vulnérabilité
3. Particularités de l’IoT
4. 3 cas concrets à ne pas imiter
5. 3 « quick wins »
6. Modèle de menaces du TUF
7. Conclusion
8. Questions / Réponses

2.

Cycle de vie d’une vulnérabilité

Les vulnérabilités informatiques : un problème ancien, encore trop mal traité

Vulnérabilité : faiblesse dans un système d'information, permettant à un attaquant de porter atteinte à la disponibilité, l'intégrité, ou la confidentialité de ce système.

Les vulnérabilités informatiques : un problème ancien, encore trop mal traité

Vulnérabilité : faiblesse dans un système d'information, permettant à un attaquant de porter atteinte à la disponibilité, l'intégrité, ou la confidentialité de ce système.

Vulnérabilité connue : vulnérabilité ayant fait l'objet d'une publication par les autorités de la sécurité des systèmes d'information (bases CERT-FR, MITRE…).

Les vulnérabilités informatiques : un problème ancien, encore trop mal traité

Vulnérabilité : faiblesse dans un système d'information, permettant à un attaquant de porter atteinte à la disponibilité, l'intégrité, ou la confidentialité de ce système.

Vulnérabilité connue : vulnérabilité ayant fait l'objet d'une publication par les autorités de la sécurité des systèmes d'information (bases CERT-FR, MITRE…).

CVE-2014-0160
aka **Heartbleed**

CVE-2014-6271
aka **ShellShock**

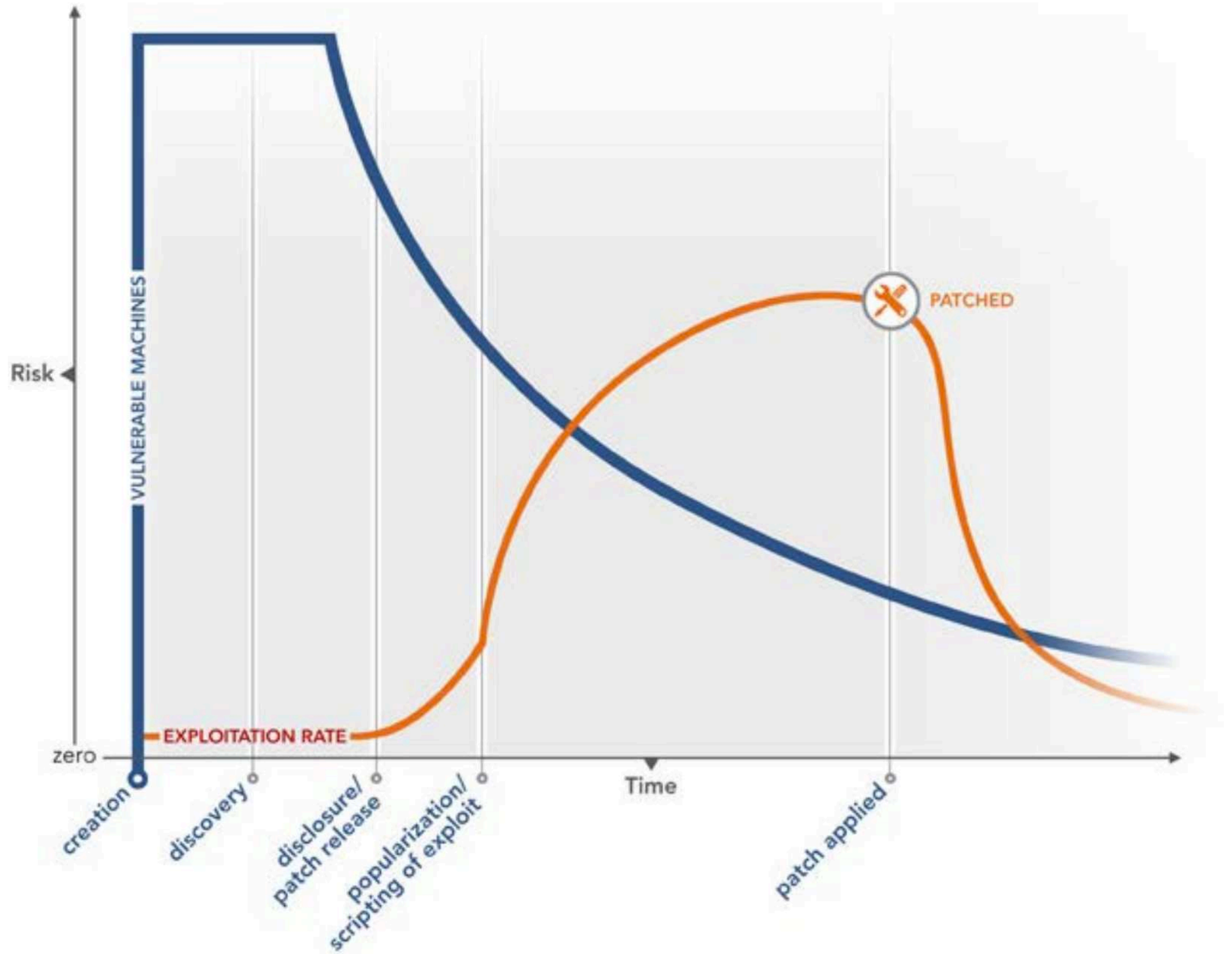
Les vulnérabilités informatiques : un problème ancien, encore trop mal traité

Gartner : d'ici 2020, 99% des vulnérabilités exploitées seront déjà connues des professionnels de la sécurité et de l'IT depuis plus d'un an.

OWASP : https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities

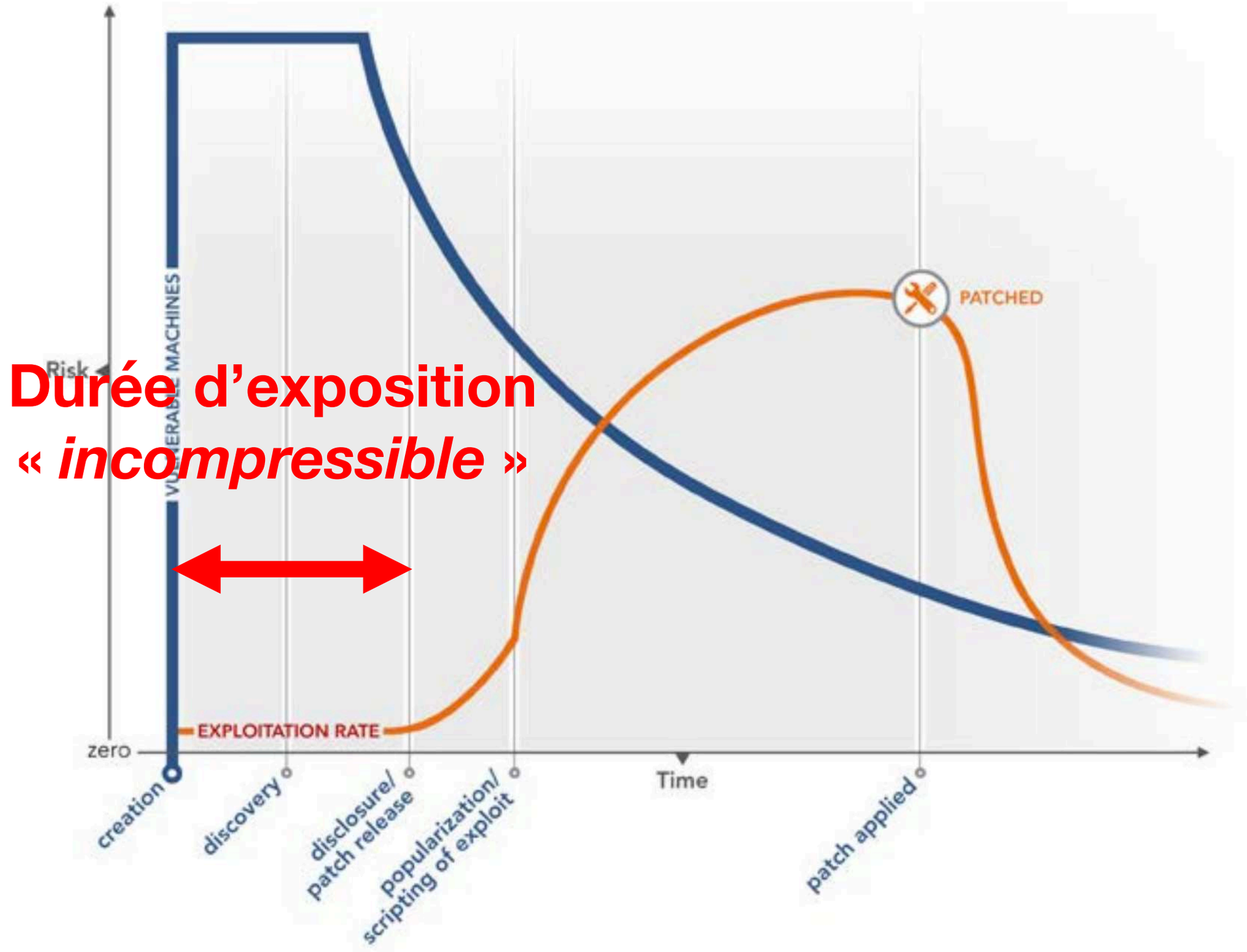
L'internet des objets sera aussi affecté.

Cycle de vie d’une vulnérabilité



Source: alertlogic.com

Cycle de vie d'une vulnérabilité

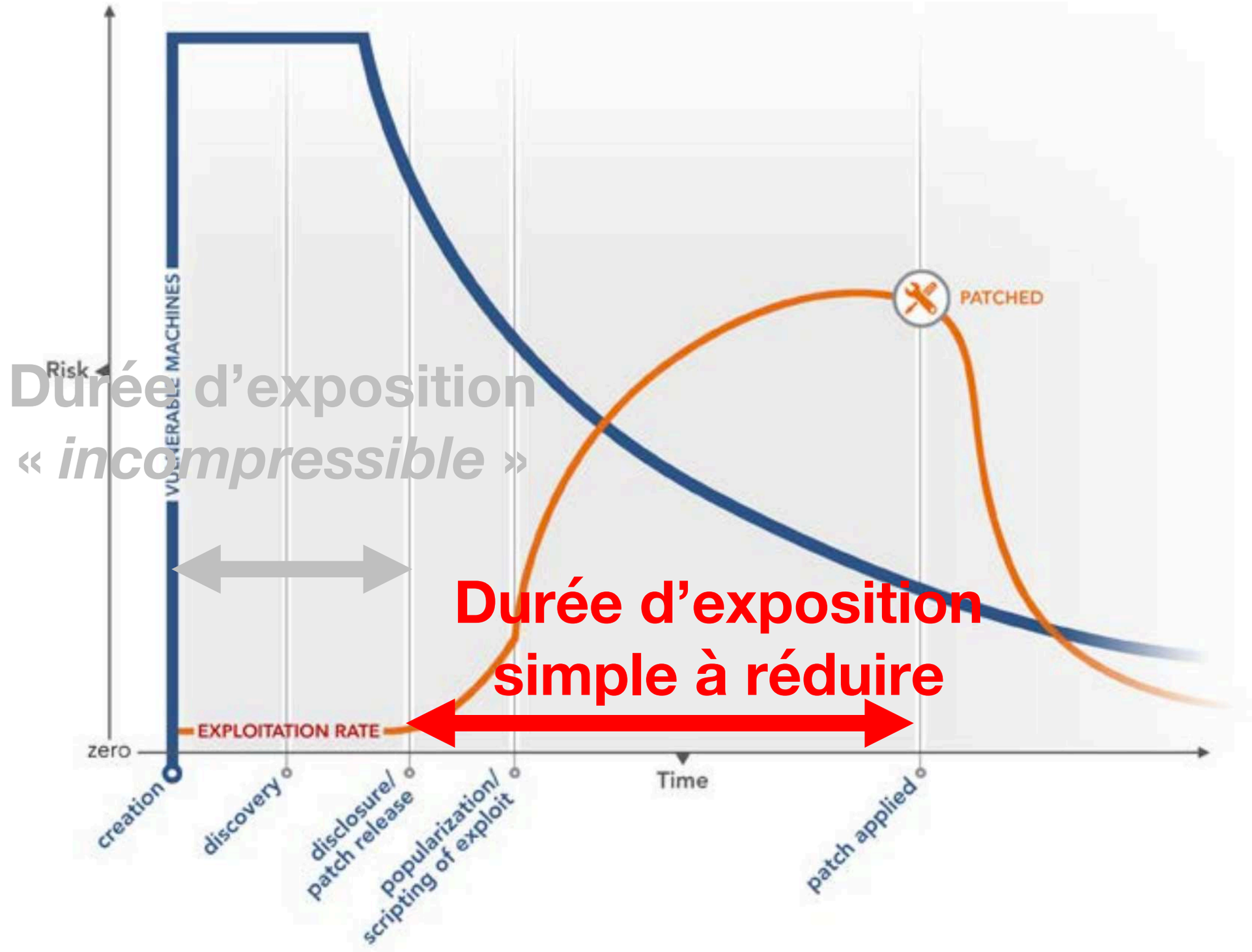


Durée d'exposition « *incompressible* »

Source: alertlogic.com

Cycle de vie d’une vulnérabilité

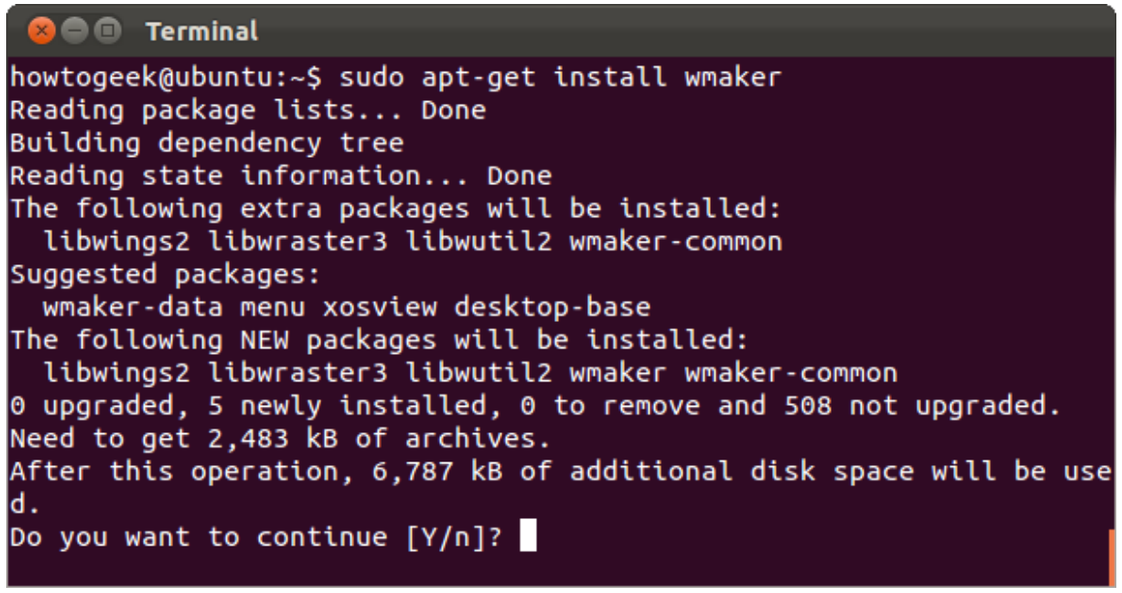
Durée d’exposition « *incompressible* »



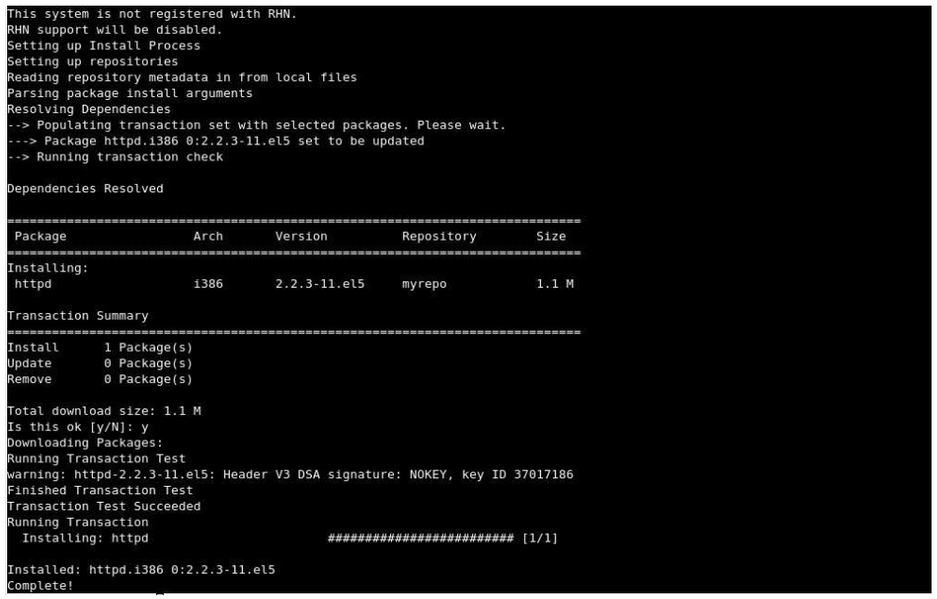
Durée d’exposition simple à réduire

Source: alertlogic.com

En pratique ?



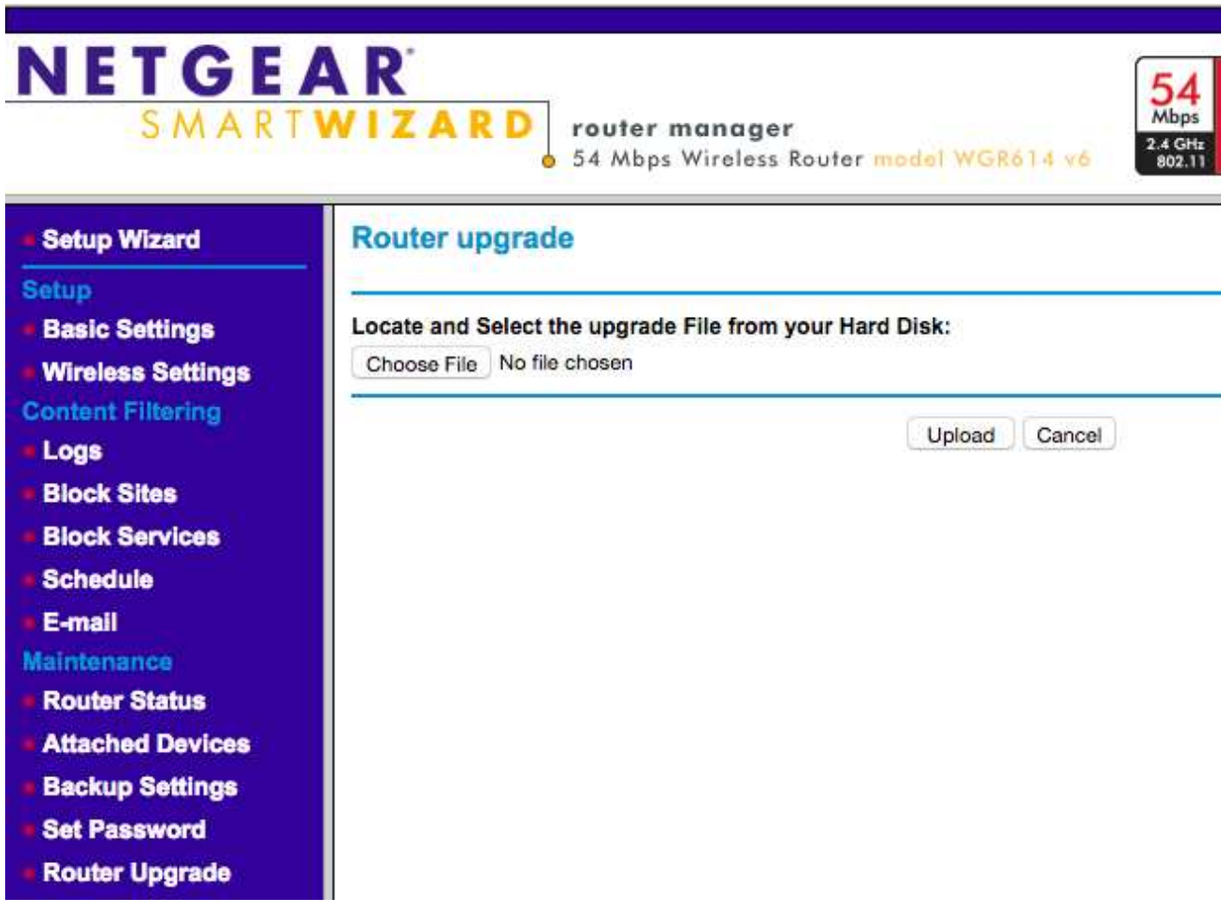
Mise à jour avec APT

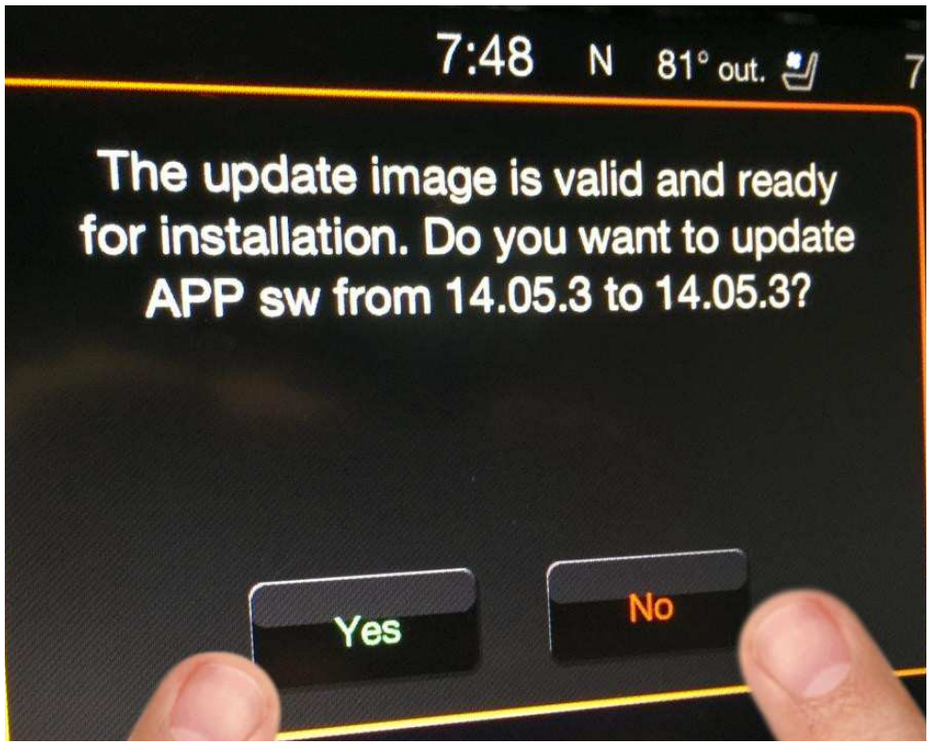


Mise à jour avec YUM

Mise à jour avec Windows Update, etc.

Mais dans l'IoT, ce n'est pas si simple…





Mais dans l’IoT, ce n’est pas si simple…

3.

Particularités de l’IoT

1. Les impacts entrent dans le monde réel :

Dégâts logiciels (vol de données)
vs. Dégâts matériels (ouverture d’une serrure connectée)

1. Les impacts entrent dans le monde réel :

Dégâts logiciels (vol de données)
vs. Dégâts matériels (ouverture d'une serrure connectée)

2. Les cycles de vie sont longs :

Cycle de vie classique ± 3 ans (ordinateur)
vs. 10 ans pour une voiture…connectée ?

1. Les impacts entrent dans le monde réel :

Dégâts logiciels (vol de données)
vs. Dégâts matériels (ouverture d'une serrure connectée)

2. Les cycles de vie sont longs :

Cycle de vie classique ± 3 ans (ordinateur)
vs. 10 ans pour une voiture…connectée ?

3. Ces systèmes sont faits pour être autonomes :

Ordinateurs, serveurs, logiciels ont
une IHM avancée et fréquemment consultée
vs. la console d'un routeur ?

Nous ne sommes pas encore habitués à patcher de tels systèmes en tant qu'usagers.

Nous ne sommes pas encore habitués à patcher de tels systèmes en tant qu'usagers.

Seuls les professionnels de la sécurité suivent les alertes sur les vulnérabilités.

Nous ne sommes pas encore habitués à patcher de tels systèmes en tant qu'usagers.

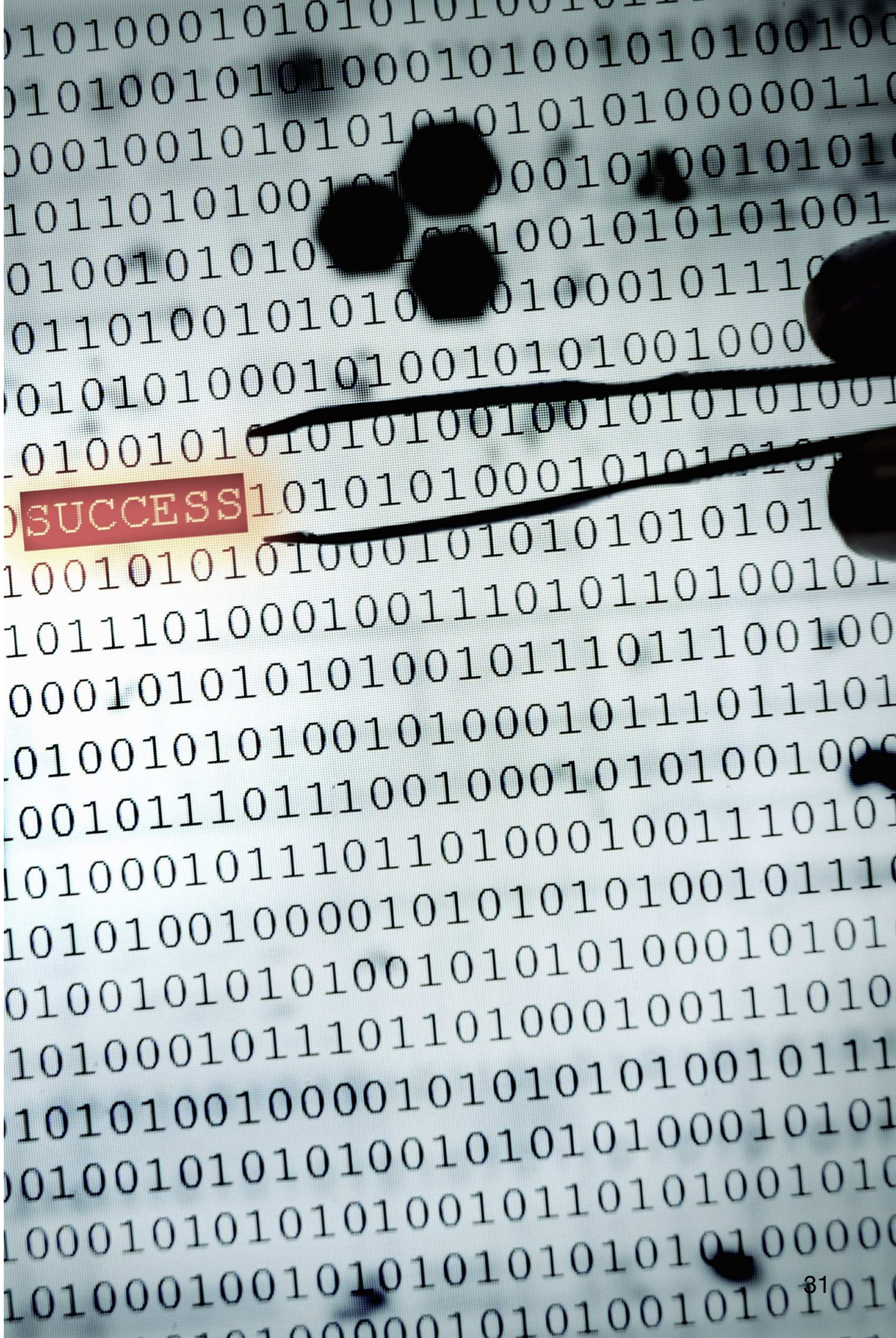
Seuls les professionnels de la sécurité suivent les alertes sur les vulnérabilités.

Il semble difficile de demander à chacun de déployer une mise à jour de sécurité sur son réfrigérateur connecté…

Dans l’IoT, la gestion des vulnérabilités doit être intégrée « by design » et par le constructeur.

4.

3 cas concrets à ne pas imiter



Cas #1 : piratage de FossHub (2 août 2016)

- FossHub est une plateforme majeure de distribution de logiciels open source.

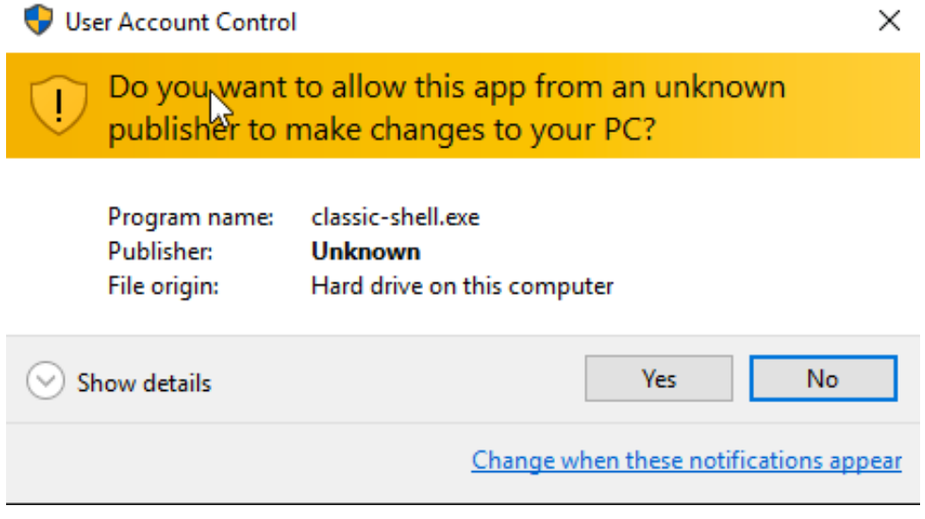
- Le 2 Août, déploiement de Windows 10 Anniversary Update.

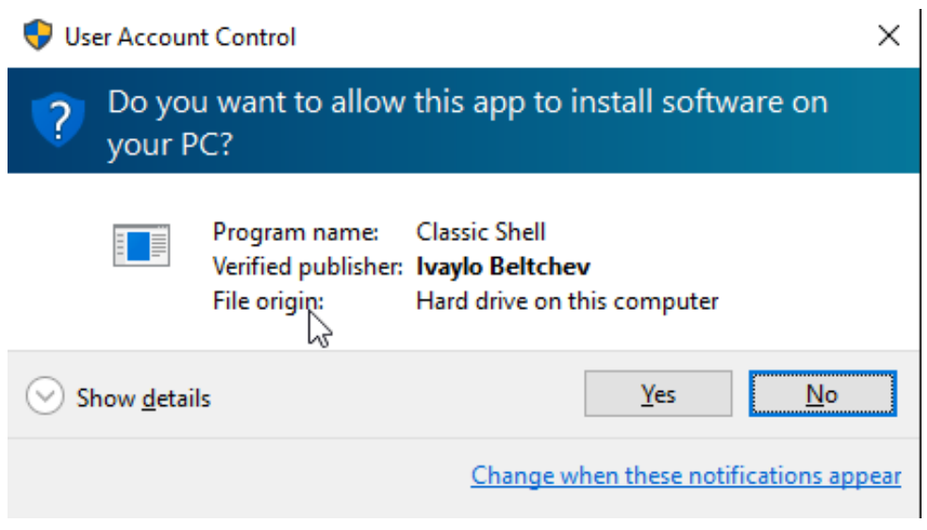
- Cette mise à jour désinstalle ClassicShell, un outil de productivité et d'ergonomie sur Windows.

- Des centaines de milliers d'utilisateurs vont sur FossHub pour télécharger et réinstaller ClassicShell.

Cas #1 : piratage de FossHub (2 août 2016)

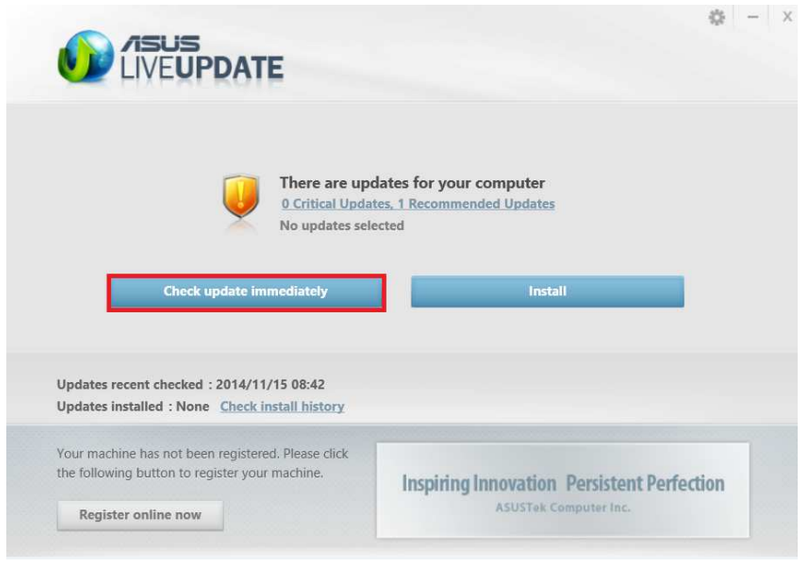
- Problème : le groupe PeggleCrew a remplacé les fichiers de FossHub par des malwares.
- Plusieurs centaines de machines infectées, bien que l'installeur corrompu n'ait pas été signé…





Signer les mises à jour n'est pas suffisant si vous demandez la validation de l'utilisateur moyen.

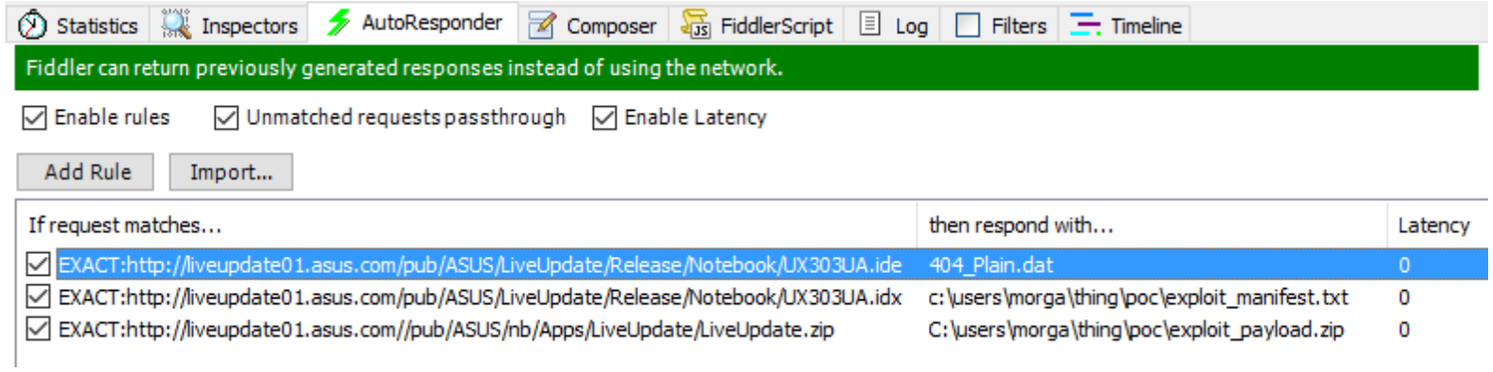
Cas #2 : ASUS Live Update

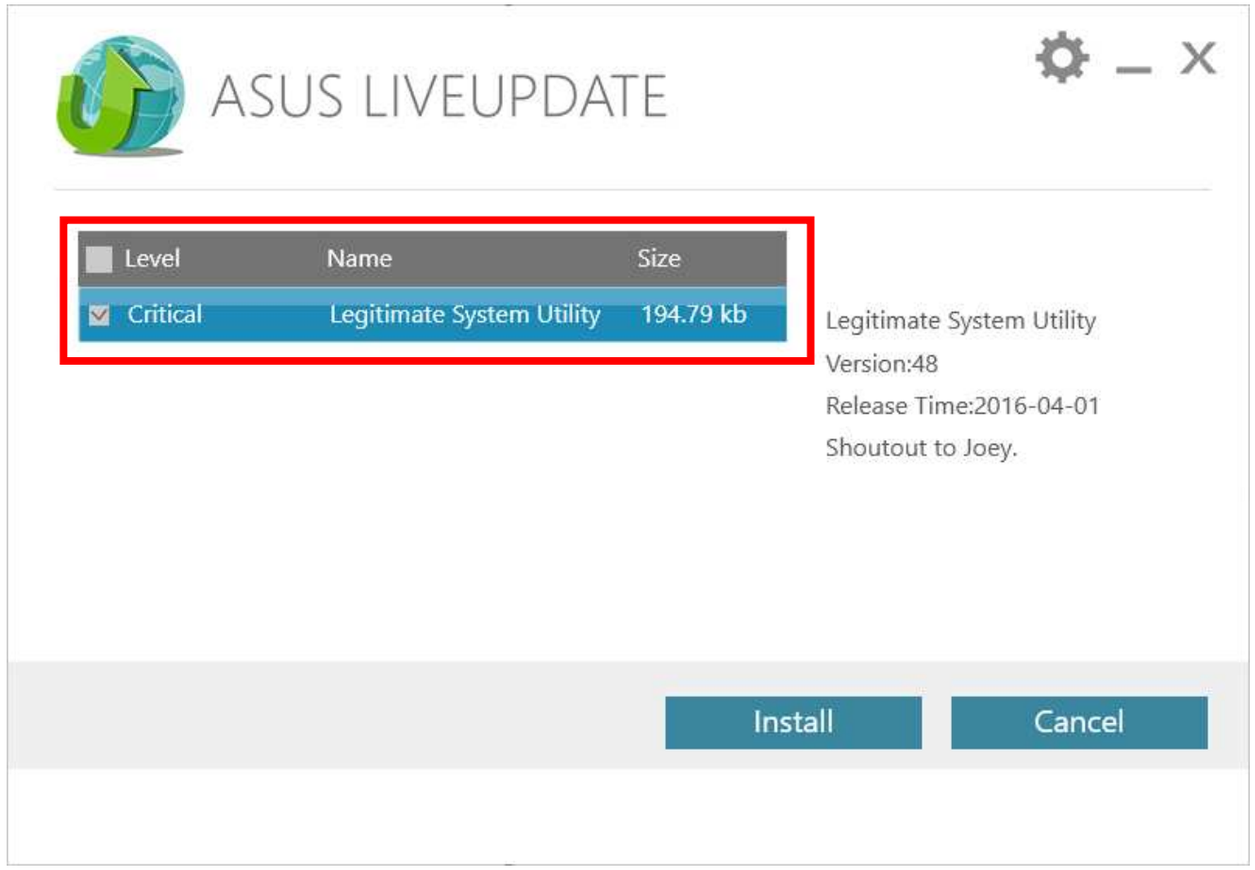


- ASUS Live Update est un logiciel de recherche et déploiement de mises à jour sur les ordinateurs ASUS.
- Les mises à jour sont exécutées par un compte à privilèges.
- Problème : l'origine des mises à jour n'est pas vérifiée, et la communication est réalisée en clair.

Cas #2 : ASUS Live Update

- Il est possible d'intercepter le trafic du logiciel, et de lui faire installer un programme malveillant.





Un dispositif de mises à jour automatisé doit vérifier l'authenticité et l'intégrité des données téléchargées.

Cas #3 : le rappel de Fiat Chrysler

- Charlie Miller et Chris Valasek divulguent de nombreuses vulnérabilités en 2015 affectant les véhicules de Fiat Chrysler.

- Fiat rappelle 1.400.000 véhicules pour les patcher.

Statement: Software Update

July 24, 2015 , Auburn Hills, Mich. - FCA US LLC is conducting a voluntary safety recall to update software in approximately 1,400,000 U.S. vehicles equipped with certain radios.

Vos systèmes doivent pouvoir être patchés à distance, sous peine de surcoûts très importants.

5.

3 « quick-wins »

Lutter contre les vulnérabilités et protéger ses usagers par 3 moyens simples

1. Monitorez les versions des logiciels déployés sur vos objets connectés.

Lutter contre les vulnérabilités et protéger ses usagers par 3 moyens simples

1. Monitorez les versions des logiciels déployés sur vos objets connectés.

2. Supervisez en continu les vulnérabilités des logiciels tiers que vous utilisez, et de vos propres systèmes.

Lutter contre les vulnérabilités et protéger ses usagers par 3 moyens simples

1. Monitorez les versions des logiciels déployés sur vos objets connectés.

2. Supervisez en continu les vulnérabilités des logiciels tiers que vous utilisez, et de vos propres systèmes.

3. Pensez dès le départ à des solutions simples et sécurisées pour patcher vos systèmes à distance.

Quelques ressources complémentaires

OWASP IoT Project :
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

The Update Framework :
https://theupdateframework.github.io/

6.

Le modèle de menaces du TUF

Le modèle de menaces générique d'un système de mises à jour (issu du TUF)

Résumé	Détails de la menace
Installation de fichiers arbitraires	L'attaquant peut installer les fichiers de son choix sur le système.
Envoi de données sans fin	L'attaquant peut envoyer des fichiers très volumineux sur le système et non gérés par ce dernier.
Installation de fausses dépendances	L'attaquant peut forcer le système à installer des logiciels tiers en les faisant passer pour des dépendances.
Attaque par avance rapide	L'attaquant fait croire au système qu'il est en avance par rapport au serveur central de mise à jour.
Attaque par gel des requêtes	L'attaquant envoie des données obsolètes au système et l'empêche de communiquer avec le serveur central, sans qu'il ne s'en rende compte.
Faux miroirs	L'attaquant se fait passer pour un miroir du serveur central et empêche le système de faire les mises à jour depuis le serveur légitime.

Le modèle de menaces générique d'un système de mises à jour (issu du TUF)

Résumé	Détails de la menace
Attaque par « mix-and-match »	L'attaquant trompe le système en générant des meta-données (ex : signatures/timestamps) et en les faisant exister plus longtemps que prévu.
Rollbacks / Downgrade	L'attaquant peut forcer le système à installer une mise à jour plus ancienne.
Ralentissement des téléchargements	L'attaquant interfère dans les communications du système et ralentit les téléchargements de sorte à gagner du temps dans ses attaques.
Accès à des clés compromis	L'attaquant obtient l'accès à des clés du système en un nombre suffisamment grand pour signer des données comme étant légitimes.
Installation d'un faux logiciel	L'attaquant envoie au système un fichier réputé de confiance mais n'étant pas le fichier attendu.

Conclusion

Intégrez la gestion et la supervision des vulnérabilités de votre système dans votre maintenance.

Conclusion

Intégrez la gestion et la supervision des vulnérabilités de votre système dans votre maintenance.

Anticipez et automatisez au maximum, dans le respect des contraintes de sécurité
(pensez au modèle de menaces du TUF).

Conclusion

Intégrez la gestion et la supervision des vulnérabilités de votre système dans votre maintenance.

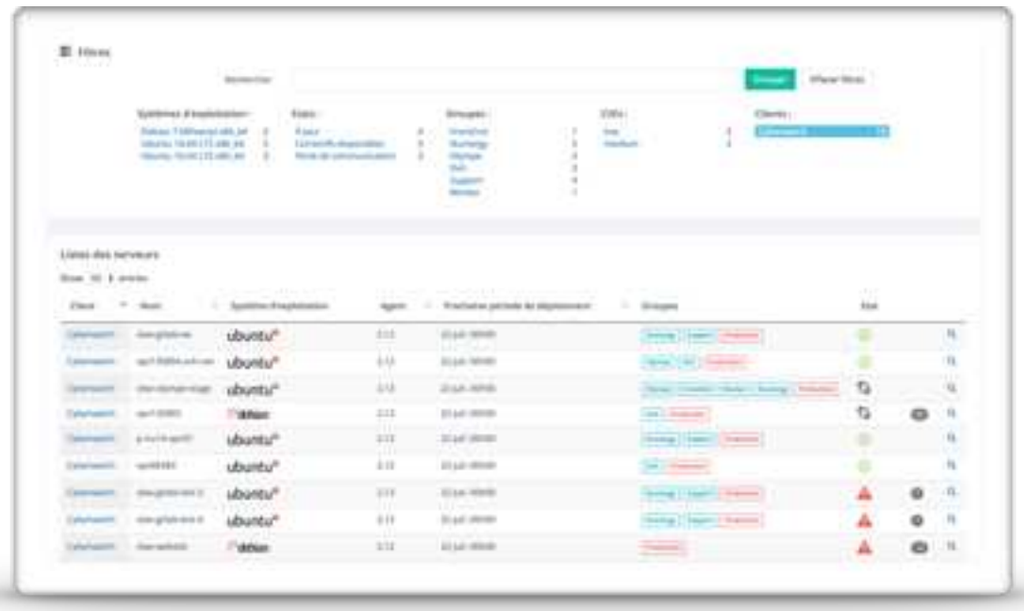
Anticipez et automatisez au maximum, dans le respect des contraintes de sécurité
(pensez au modèle de menaces du TUF).

Votre capacité à répondre à un incident de sécurité sera décuplée par votre capacité à patcher vos systèmes.

Questions / Réponses

Merci pour votre attention !

Cyberwatch



Logiciel de détection et supervision des vulnérabilités.

Demandez une démonstration !

www.cyberwatch.fr