
# Sécurité des produits Red Hat

## Mieux comprendre et mitiger les failles de sécurité

Karim Roukoz
Architecte de Solutions Senior
kar@redhat.com

Red Hat

# AGENDA

- Rapport des risques 2018
- La vision de sécurité des produits Red Hat
- La gestion et la classification des vulnérabilités
- “Customer Security Awareness Events”
- Pop Quiz

Red Hat


IN 2018
745
Red Hat
SECURITY ADVISORIES
1,272
CVEs
ADDRESSED
Source: 2018 Red Hat Product Security Risk Report, February 2019. red.ht/2018riskreport

Red Hat

# Rapport des risques 2018

- 1,272 CVEs ont été adressé en 2018, une augmentation de 11% comparé à 2017
- 745 Avis de Sécurité Red Hat émis, une augmentation en continu année après année
- 3,774 problèmes de sécurité ont été communiqué à l'équipe de Sécurité des Produits Red Hat (environ x2 comparé à 2015)
- 111 avis de sécurité critiques adressant 57 vulnérabilités Critique
    - 75 RHEL, 15 Middleware, 20 OCP, 0 OCP
- 80% des problèmes critiques ont été adressé en 1 semaine
- 38% des problèmes critiques ont été adressé en 1 jour ouvrable

https://red.ht/2018riskreport

Red Hat

# La vision de sécurité des produits Red Hat

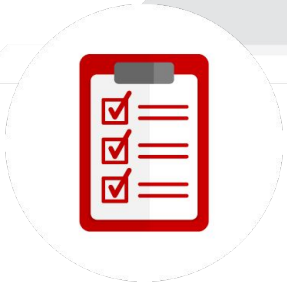
“Nous croyons que tout le monde, partout à droit à des informations de qualité nécessaire pour atténuer les risques de sécurité et d’atteinte aux renseignements personnels. Nous luttons pour protéger les communautés de clients, de contributeurs, et de partenaires des menace de sécurité numérique. Nous croyons que les principes du logiciel libre sont les meilleurs pour y aboutir.”

Red Hat

# Sécurité des produits Red Hat

L’équipe de sécurité des produits Red Hat travaille constamment pour assurer des correctif et donner une réponse rapide quant à la résolution des problèmes.

## Notre équipe assure la sécurité de produits et services à travers:



L’investigation des problèmes et l’identification des produits affectés

L'évaluation de l’impact

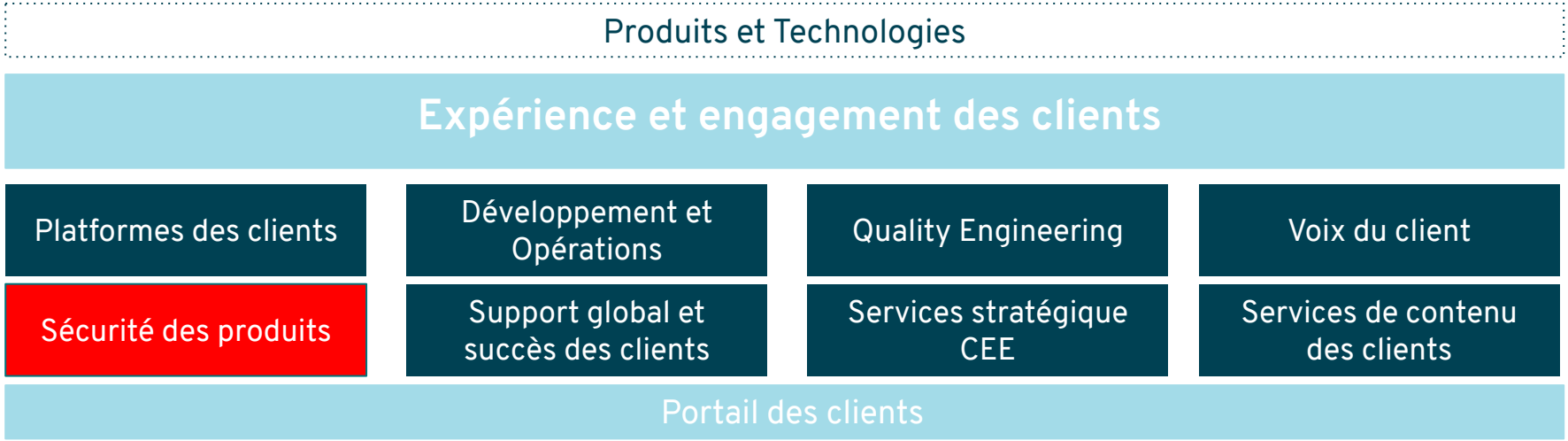
La détermination des correctifs nécessaires

La communication des problèmes et des correctifs aux clients

Red Hat

# Expérience et Engagement des Clients

L'équipe d'Expérience et Engagement des Clients (CEE) est la voix des clients au niveau "Engineering" de Red Hat.




Red Hat

# Qu’est ce qu’une faille de sécurité?

Une faille de sécurité est une faiblesse dans un logiciel, firmware ou matériel informatique qui pourrait permettre à un attaquant d'interagir avec un système d’une manière dont il n’est pas supposé. (Source: Wikipedia)

Les failles qui nous tiennent éveillées la nuit sont celles qui:

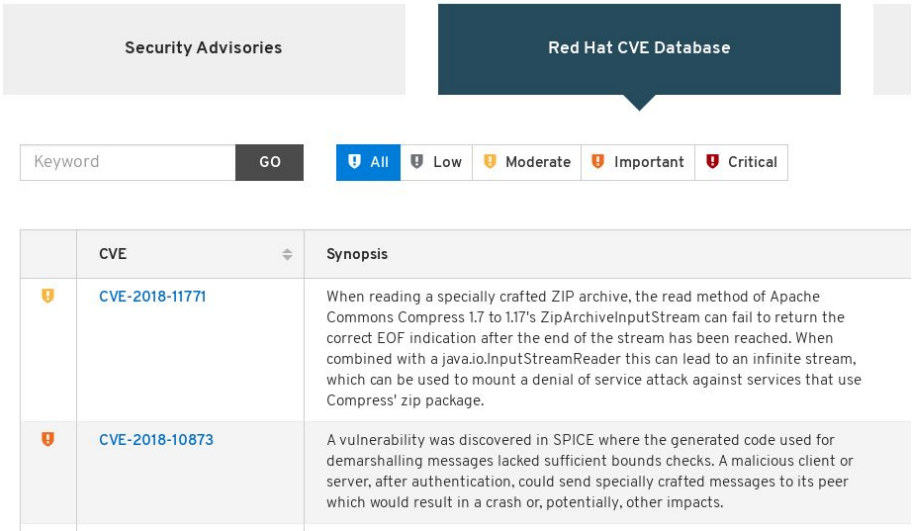
- compromettent des donnés sensibles (informations financières, information clients privées)
- permettent l'exécution de code arbitraire sur des systèmes distants
- causent un déni de services critiques (DoS)

La sévérité d’une faille est déterminée par:

- la probabilité que la faille soit exploitée
- l’impact aux systèmes ou aux biens exposés
- la valeur des systèmes ou des biens

Red Hat

# Common Vulnerabilities and Exposures (CVE)




Les CVE fournissent une façon transparente d'identifier et suivre des problèmes de sécurité

- L'équipe de sécurité des produits Red Hat attribue un CVE à chaque problème de sécurité qui impacte nos produits
- Un CVE peux être assigné rétroactivement à des bugs dont l'impacte de sécurité est décelé après la découverte du bug
- Tous les CVE relatifs aux produits Red Hat sont publiés dans nos bases de données publiques

https://access.redhat.com/security/security-updates/#/cve

Red Hat

# Vue approfondie des CVEs

Les CVEs ont un identifiant unique

*CVE-2019-5736*

Les CVEs incluent une description brève

*runc: Execution of malicious containers allows for container escape and access to host filesystem*

Les CVEs incluent des réferences pertinentes

*https://access.redhat.com/security/cve/cve-2019-5736*

*https://bugzilla.redhat.com/show_bug.cgi?id=1664908*

https://cve.mitre.org/about/index.html

Red Hat

# Les CVEs “branded”

*Connaissez vous CVE-2014-0160?*

Heartbleed

https://cve.mitre.org/about/index.html

Red Hat

# Common Vulnerability Scoring System (CVSS)

## Déterminez le score de initial

Il y'a 8 facteurs à prendre en compte

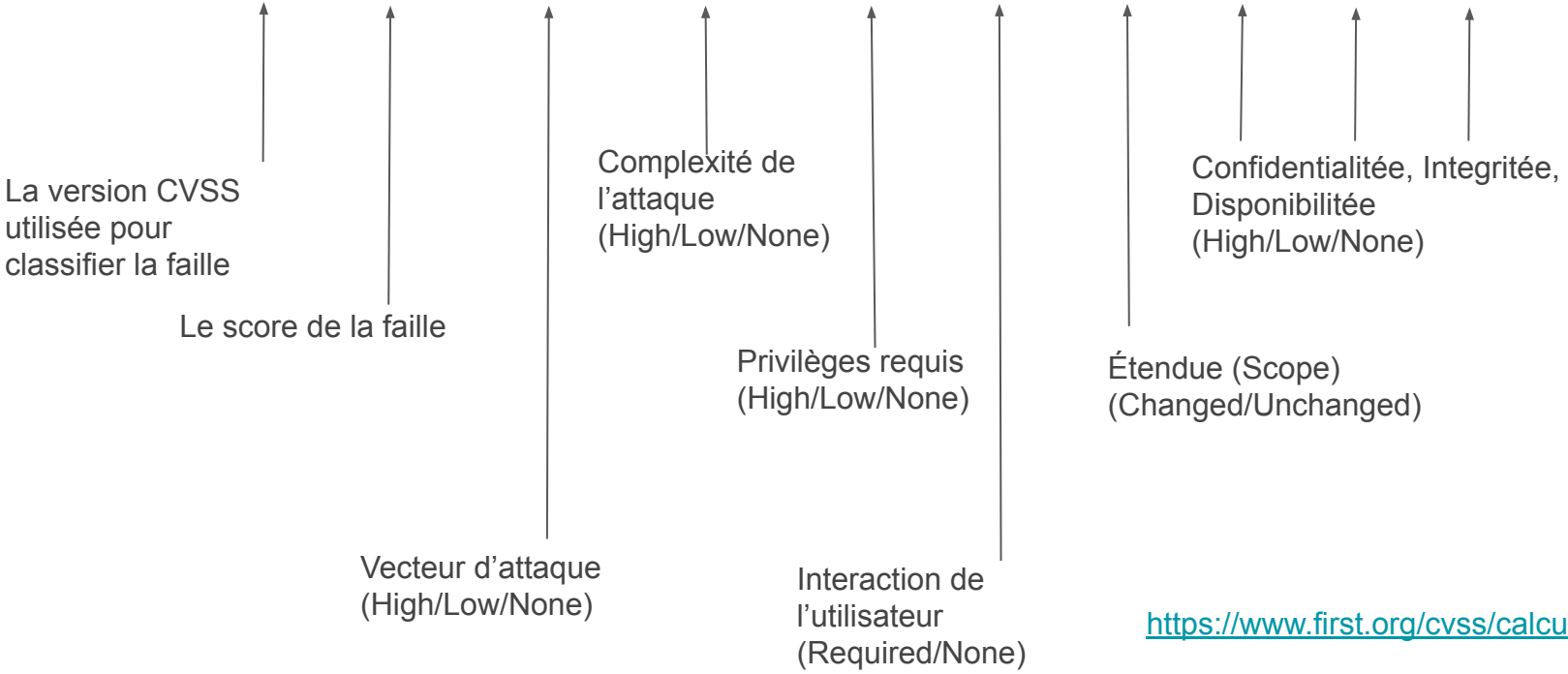
- Vecteur d'attaque
- Complexité de l'attaque
- Privilèges requis
- Interaction de l'utilisateur
- Étendue
- Confidentialité
- Integrité
- Disponibilité

Chaque facteur est classifié sur une échelle de Haute-Basse-Nul

Astuce de pro: Vous pouvez personnaliser le score pour vos environnements

# Comment lire un CVSS

CVSS:3.0- 7.7/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H




https://www.first.org/cvss/calculator/3.0

Red Hat

# Provenance des scores

**National Vulnerability Database - NVD** *vs* **Red Hat**

La faille n’est pas évaluée par un expert dans la technologie

L'évaluation ne tient pas en compte des facteurs tel que les paramètres de compilation, les renforcements des systèmes, ou des outils tel que SELinux

Pas de tests effectué pour reproduire la faille dans des environnements représentatifs

L’évaluation générique ne tient pas en compte les différents paramètres du système d’exploitation

La faille est évaluée par des spécialistes en sécurité des produits Red Hat

L’évaluation prend en compte les facteurs de “build” et les paramètres utilisés par Red Hat

L’évaluation reflète les essais réels et le triage des problèmes sur les produits impactés

L’évaluation est spécifique aux paramètres du système d’exploitation

Red Hat

# Exemple de personnalisation

*CVE-2019-5736: runc: Execution of malicious containers allows for container escape and access to host filesystem*

## Common Vulnerability Scoring System (CVSS) Score Details

CVSS v3 Score Breakdown

| | Red Hat | NVD |
|---|---|---|
| **CVSS v3 Base Score** | 7.7 | 8.6 |
| **Attack Vector** | Local | Local |
| **Attack Complexity** | High | Low |
| **Privileges Required** | None | None |
| **User Interaction** | Required | Required |
| **Scope** | Changed | Changed |
| **Confidentiality** | High | High |
| **Integrity Impact** | High | High |
| **Availability Impact** | High | High |

CVSS v3 Vector

**Red Hat:** CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

**NVD:** CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

https://access.redhat.com/security/cve/cve-2019-5736

Red Hat

# CVSS != RISQUE

# Le CVSS détermine la sévérité

Le CVSS est un des points à surveiller dans l'évaluation des risques.

Red Hat prend en compte d'autres facteurs:

- La faille s'applique-elle aux produits Red Hat?
- Comment le code a été livré dans les produits Red Hat (compiler flags, etc)?
- Y a-t-il des mécanismes existants (ex. SELinux) qui réduisent le risque?

# L’importance des CVSS

Les scores CVSS fournissent une méthode de priorisation des vulnérabilités.

Quels autres facteurs doivent être pris en compte par nos clients?

- Où et comment sont déployés les produits affectés
- Les compromis de sécurité versus l'évaluation des risques
- Les requis de conformité réglementaire versus les risques réels

Red Hat

# Classement de sévérité Red Hat

### Critique

Un utilisateur distant non-authentifié peut exécuter du code arbitraire

Ne nécessite pas d'interaction avec l'utilisateur

### Important

Un utilisateur local peut obtenir des privilèges élevés

Un utilisateur distant non-authentifié peut accéder à des ressources en mode lecture

Un utilisateur distant non-privilégié peut exécuter du code arbitraire

### Moderée

L'exploit est difficilement atteignable

Exploitable via des paramètres non commun et peu probable

### Faible

Des circonstances peu probable sont requises pour exploiter la faille

L'impact est minime en cas d'exploit

https://access.redhat.com/security/updates/classification/

Red Hat

# Que faire si vous trouvez une faille?

Si vous pensez avoir trouvé une faille de sécurité, contactez l'équipe de sécurité des produits à l'adresse courriel suivante secalert@redhat.com

L'équipe de sécurité des produits analysera et gérera les rapports reçus.

En cas de faille dans des projets “upstream”, l'équipe de sécurité des produits de Red Hat aidera dans la coordination des discussions et imposera un embargo médiatique si nécessaire

Red Hat

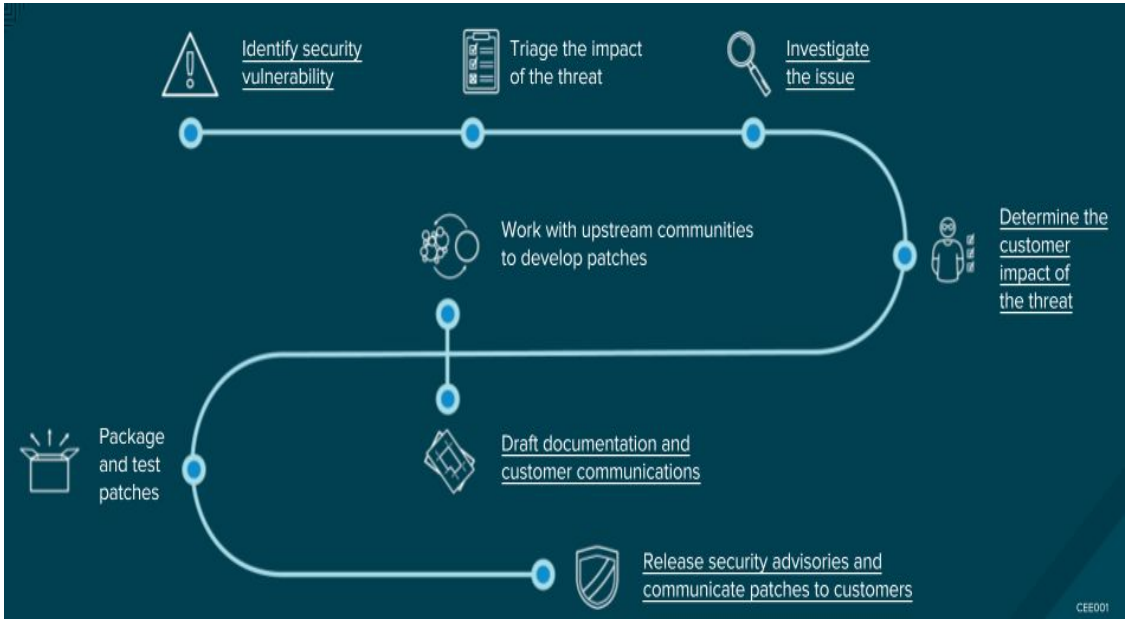
# Divulgation coordonnée des vulnérabilités

- Red Hat fait parti d'un groupe de fournisseurs et d'équipes spécialisées en sécurité dans la communauté
- Nous utilisons un processus nommé Coordinated Vulnerability Disclosure
- Le but est de protéger les clients et les communautés globales
- Red Hat travaille avec le rapporteur de la faille pour établir la démarche corrective, et la durée de l'embargo médiatique

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Red Hat

# Customer Security Awareness events (CSAw)




Le CSAw est un processus spécialisé pour gérer des situations critiques:

- Faille de sévérité critique ou importante
- Forte attention médiatique
- Exploitation active de la faille

Le processus CSAw assure:

- Une résolution rapide
- La communication transparente et exhaustive envers les clients (Courriel, portail des clients, Red Hat Insights)

https://access.redhat.com/articles/2968471

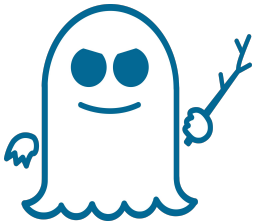
Red Hat

# Ne croyez pas au battage médiatique

- Une vulnérabilité peut avoir un nom, un logo, ou l'attention de la presse, ceci n'équivaut pas à un risque plus élevé
- Red Hat peut vous guider à travers les vulnérabilités qui méritent votre attention immédiate, et celles qui ont des risques moins sévères que leur réputation médiatique

Drown

Meltdown



Spectre

Foreshadow

Shellshock

Badlock

Heartbleed

Red Hat

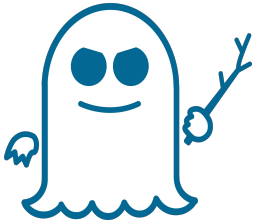
# POP QUIZ!!!

- Combien de ces failles ont été classifié **Critique** par Red Hat?

  Ne croyez pas au battage médiatique. Elles sont toutes classées Importantes, sauf une.

Drown

Meltdown



Spectre

Foreshadow

Shellshock

Badlock

Heartbleed

Red Hat

# POP QUIZ!!!

CVE-2014-6271 Shellshock

https://access.redhat.com/security/vulnerabilities/shellshock

# Merci!