

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

# De la vulnérabilité à la crise

S. de Maupeou - CERTA - [www.certa.ssi.gouv.fr](http://www.certa.ssi.gouv.fr)

Forum du CERT IST 12 juin 2008

# Plan de la présentation

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 De quoi s'agit-il ?**
  - Les vulnérabilités
  - Les crises
- 2 Histoires de vulnérabilités**
  - JetDataBase
  - OpenSSL/Debian
  - Flash
- 3 Tentatives d'approche rationnelle**
  - Mesures d'impact ?
  - Enseignements
- 4 Conclusion**

# Caractéristiques d'une vulnérabilité ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Une information fragilisant le SI qui peut-être :
  - technique (exemple `openssl` sous Debian) ;
  - organisationnelle (pas de politique de mise à jour des correctifs) ;
  - connue ou pas (0day).

# Caractéristiques d'une vulnérabilité ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Une information fragilisant le SI qui peut-être :
  - technique (exemple `openssl` sous Debian) ;
  - organisationnelle (pas de politique de mise à jour des correctifs) ;
  - connue ou pas (0day).
- Son impact est difficile à évaluer :
  - dépendant de l'architecture du SI ;
  - exploitation à distance ou pas ?
  - automaticité de l'exploitation ou pas ?
  - correctif disponible ou pas ?
  - version d'application vulnérable ?

# Quelques constats sur les crises !

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités

Les crises

### Histoires de vulnérabilités

JetDataBase

OpenSSL/Debian

Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?

Enseignements

### Conclusion

- Les réseaux amplifient les évènements par effet de levier.
- Le fonctionnement même de nos sociétés est de plus en plus lié aux SI.
- La société de l'information s'est développée sur des protocoles Internet fragiles techniquement.
- Des attaques « hors limites » (territoriales, légales, capacités, etc.).

# Quelques constats sur les crises !

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités

Les crises

### Histoires de vulnérabilités

JetDataBase

OpenSSL/Debian

Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?

Enseignements

### Conclusion

- Les réseaux amplifient les évènements par effet de levier.
- Le fonctionnement même de nos sociétés est de plus en plus lié aux SI.
- La société de l'information s'est développée sur des protocoles Internet fragiles techniquement.
- Des attaques « hors limites » (territoriales, légales, capacités, etc.).
- Il y a crise notamment lorsque :
  - impacts sur le fonctionnement des organisations ;
  - les médias relaient des informations.
- Mais il y a des situations qui devraient provoquer une crise et qui ne déclenchent rien de visible !
- Pseudo crise ? Une crise est elle nécessairement visible ?

# Plan de la présentation

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 De quoi s'agit-il ?
  - Les vulnérabilités
  - Les crises
- 2 Histoires de vulnérabilités**
  - JetDataBase
  - OpenSSL/Debian
  - Flash
- 3 Tentatives d'approche rationnelle
  - Mesures d'impact ?
  - Enseignements
- 4 Conclusion

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 0Day : Alerte du CERTA le 25 mars
- Avril : cas discrets d'attaques
- 14 Mai : correctif de Microsoft

## Ingrédients de la crise

Nature de l'application mais pas d'automaticité !

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 0Day : Alerte du CERTA le 25 mars
- Avril : cas discrets d'attaques
- 14 Mai : correctif de Microsoft

## Ingrédients de la crise

Nature de l'application mais pas d'automaticité !

## Enseignement

La crise n'a pas (encore) émergé !

# OpenSSL/Debian

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 13 Mai : correctif sur le générateur pseudo-aléatoire
- Toutes les clefs depuis 2006 sont très faibles !

## Ingrédients de la crise

Concerne les secrets mais mal connue et complexe.

# OpenSSL/Debian

De la  
vulnérabilité  
à la crise

De quoi  
s'agit-il ?

Les vulnérabilités  
Les crises

Histoires de  
vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

Tentatives  
d'approche  
rationnelle

Mesures d'impact ?  
Enseignements

Conclusion

- 13 Mai : correctif sur le générateur pseudo-aléatoire
- Toutes les clefs depuis 2006 sont très faibles !

## Ingrédients de la crise

Concerne les secrets mais mal connue et complexe.

## Enseignement

La crise est latente !

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```



DEBIAN

GUARANTEED ENTROPY.

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 9 avril 2008 : correctif sur Adobe Flash Player
- 28 mai : alertes sur l'Internet à propos d'un 0Day sur Flash massivement exploité
- Analyse en profondeur du CERTA
- Publication d'une communication rationnelle.

## Ingrédients de la crise

Concerne les postes clients, relais dans les médias.

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 9 avril 2008 : correctif sur Adobe Flash Player
- 28 mai : alertes sur l'Internet à propos d'un 0Day sur Flash massivement exploité
- Analyse en profondeur du CERTA
- Publication d'une communication rationnelle.

## Ingrédients de la crise

Concerne les postes clients, relais dans les médias.

## Enseignement

La crise est contenue !

► [SecInfo](#)

# Plan de la présentation

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 De quoi s'agit-il ?
  - Les vulnérabilités
  - Les crises
- 2 Histoires de vulnérabilités
  - JetDataBase
  - OpenSSL/Debian
  - Flash
- 3 Tentatives d'approche rationnelle**
  - Mesures d'impact ?
  - Enseignements
- 4 Conclusion

# Quels critères retenir ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 Impact de la vulnérabilité/attaque ?  $F$ (déploiement, organisation, particulier, architecture) ;

# Quels critères retenir ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 Impact de la vulnérabilité/attaque ?  $F$ (déploiement, organisation, particulier, architecture) ;
- 2 Vulnérabilité/attaque relayée par les médias ?  $F$ ( ?)

# Quels critères retenir ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 Impact de la vulnérabilité/attaque ?  $F$ (déploiement, organisation, particulier, architecture) ;
- 2 Vulnérabilité/attaque relayée par les médias ?  $F$ ( ?)
- 3 Nature de la vulnérabilité/attaque ?  $F$ (automaticité, correctif, surprise, complexité)

# Quels critères retenir ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- 1 Impact de la vulnérabilité/attaque ?  $F$ (déploiement, organisation, particulier, architecture) ;
- 2 Vulnérabilité/attaque relayée par les médias ?  $F$ ( ?)
- 3 Nature de la vulnérabilité/attaque ?  $F$ (automaticité, correctif, surprise, complexité)
- 4 Capacité de gestion de crise ?  $F$ (anticipation, communication, compréhension, pédagogie)

# De la vulnérabilité à la crise ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Le passage de la vulnérabilité à la crise est très ténu et la transition est plus proche du crash d'un avion que d'une pandémie
- La gestion d'une crise SSI n'est pas du ressort exclusif des experts ! Elle relève d'une décision fondée sur les impacts possibles du risque.
- Gérer le risque SSI comme le risque de pollution : une maturité à acquérir

# De la vulnérabilité à la crise ?

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Le passage de la vulnérabilité à la crise est très ténu et la transition est plus proche du crash d'un avion que d'une pandémie
- La gestion d'une crise SSI n'est pas du ressort exclusif des experts ! Elle relève d'une décision fondée sur les impacts possibles du risque.
- Gérer le risque SSI comme le risque de pollution : une maturité à acquérir
- La transition de l'incident à la crise n'est pas une science exacte. La prise en compte par les médias peut être un bon indicateur !
- Les experts doivent communiquer et prévenir qu'ils ne se trompent sur l'impact : rien n'est pire que la surprise !

# Quand la crise est là

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Les plans gouvernementaux spécialisés prévoient la mise en place de deux structures de gestion de crises :
  - **ad hoc** : cellule interministérielle de crise chargée de préparer les prises de décisions qui relèvent de l'autorité politique ;
  - **permanente** : centre opérationnel chargé de la conduite de l'action.

# Quand la crise est là

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Les plans gouvernementaux spécialisés prévoient la mise en place de deux structures de gestion de crises :
  - **ad hoc** : cellule interministérielle de crise chargée de préparer les prises de décisions qui relèvent de l'autorité politique ;
  - **permanente** : centre opérationnel chargé de la conduite de l'action.
- La SSI au travers des plans de vigilance et de réaction s'est inscrite dans cette logique de gestion de crise au moyen du **Centre Opérationnel de la SSI (COSSI)**.
- Cela se prépare en particulier par des exercices.

# Le COSSI

De la vulnérabilité à la crise

De quoi s'agit-il ?

Les vulnérabilités  
Les crises

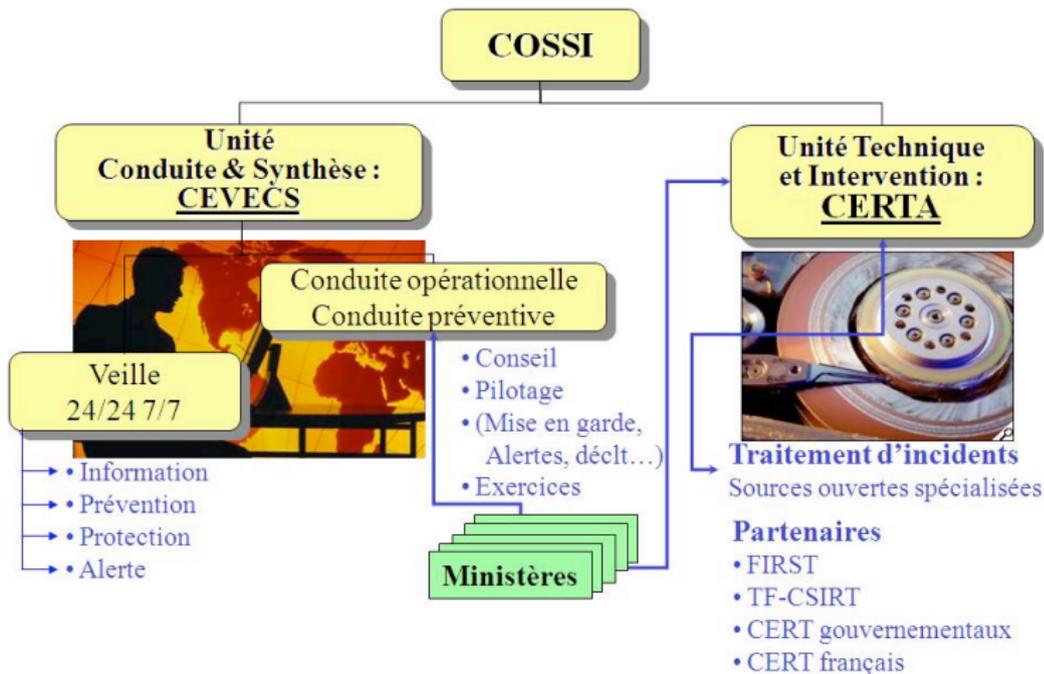
Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

Conclusion



# Enseignements

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?

### Enseignements

### Conclusion

- Les conséquences des attaques : une réflexion dépendante de la maîtrise du SI (cartographie).
- Les aspects pénaux et juridiques sont encore très largement à approfondir.
- La communication de crise est une des clefs de sa gestion.

# Enseignements

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?

### Enseignements

### Conclusion

- Les conséquences des attaques : une réflexion dépendante de la maîtrise du SI (cartographie).
- Les aspects pénaux et juridiques sont encore très largement à approfondir.
- La communication de crise est une des clefs de sa gestion.
- Le temps de l'expert, le temps du juriste, le temps de la presse : pas toujours facile de trouver un point de rencontre !
- Chacun son rôle : les experts proposent des mesures techniques et les décisions intègrent l'impact possible sur la population.
- Quand la crise est là, l'informatique est un vecteur mais l'impact est d'abord sociétal ou organisationnel.

# La supervision : un impératif insuffisant

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?

Enseignements

### Conclusion

- Les attaques réussies sont des attaques surprises : un centre de supervision de la sécurité permet d'atténuer l'inévitable panique.
- Quand l'attaque est visible le mal est déjà fait, mais traiter les conséquences n'est pas suffisant !
- Un centre de supervision peut apporter une certaine rationalité.

# La supervision : un impératif insuffisant

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Les attaques réussies sont des attaques surprises : un centre de supervision de la sécurité permet d'atténuer l'inévitable panique.
- Quand l'attaque est visible le mal est déjà fait, mais traiter les conséquences n'est pas suffisant !
- Un centre de supervision peut apporter une certaine rationalité.
- Le suivi des correctifs et le suivi des parcs est **le** point clef.
- Les limites :
  - perception et compréhension que la crise est naissante : savoir «passer la main» ;
  - gestion de la communication et de l'impact des mesures correctives.

# Tout faire pour que les crises ne se produisent pas et prévoir que cela arrive

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Mesurer et tester sa capacité de travail en mode dégradé.
- Politique de mise à jour : connaître son parc et se doter d'une capacité et d'une légitimité pour appliquer un correctif.
- Faire appel à des professionnels pour estimer le niveau de protection et traiter les incidents.
- Se doter d'une capacité de supervision de la sécurité pour traiter l'incident informatique, appréhender la crise informatique puis aider à la gestion de la crise.
- S'ENTRAINER !!!

# Encore beaucoup d'inconnues !

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Réunir des compétences variées pour faire face à des crises dont l'ampleur reste une inconnue.
- En amont, exploiter une supervision pour détecter, entraîner, prévoir, sensibiliser.
- Suivre les vulnérabilités, mesurer les risques dans le report d'application d'un correctif.

# Encore beaucoup d'inconnues !

## De la vulnérabilité à la crise

### De quoi s'agit-il ?

Les vulnérabilités  
Les crises

### Histoires de vulnérabilités

JetDataBase  
OpenSSL/Debian  
Flash

### Tentatives d'approche rationnelle

Mesures d'impact ?  
Enseignements

### Conclusion

- Réunir des compétences variées pour faire face à des crises dont l'ampleur reste une inconnue.
- En amont, exploiter une supervision pour détecter, entraîner, prévoir, sensibiliser.
- Suivre les vulnérabilités, mesurer les risques dans le report d'application d'un correctif.
- Prévoir le 0Day : c'est à dire prévoir l'imprévisible.
- Chercher les facteurs d'équilibre dans l'environnement instable des crises.
- Les médias vont souvent (toujours ?) plus vite que le gestionnaire de crise qui risque de rester figé sur les aspects techniques

# Portail de la Sécurité informatique

Présentation | Dernières modifications | Glossaire | Les dix commandements | Recherche

## Je suis...

Particulier  
Entreprise

## Je cherche...

Autoformation  
Fiche technique  
Guide de configuration  
Mémento  
Question / Réponse  
Une solution pour me protéger  
Lien

## Actualités

Alertes  
Faits marquants  
Technique

## Alertes

### Exploitation massive d'une vulnérabilité liée à la technologie Flash

Des vulnérabilités du lecteur Flash de l'éditeur Adobe sont actuellement massivement exploitées sur le réseau Internet.

Ce lecteur est intégré à la plupart des navigateurs web et permet de visualiser les animations écrites dans ce format (comme par exemple des vidéos ou des présentations animées). L'exploitation de ces vulnérabilités permet à une personne malveillante de prendre le contrôle à distance de l'ordinateur de sa victime ou à un code malveillant de s'exécuter automatiquement à l'ouverture de l'une de ces animations Flash.

Cette vague d'attaques est dangereuse car elle se propage par la simple navigation des internautes sur le web sans qu'ils aient besoin de cliquer sur un lien particulier. De plus, la mise à jour Flash n'est pas toujours automatique et peut requérir une action de l'internaute.

En l'état actuel des informations dont nous disposons, ces vulnérabilités sont corrigées.

### INTERNAUTES :

Pour ne plus être vulnérable, il convient de procéder aux actions suivantes :

- ▶ mettez à jour le module Flash : les téléchargements sont disponibles directement sur le site de l'éditeur **Adobe** ;
- ▶ mettez à jour votre logiciel anti-virus ;
- ▶ il est par ailleurs recommandé de ne pas activer l'exécution des codes JavaScript par défaut.

## PARTENAIRES



**DCSSI**  
Site thématique de la sécurité des systèmes d'information.



**Délégation aux usages de l'Internet**  
Pour rendre l'Internet plus sûr et plus accessible à tous



**OCLCTIC**  
Animer et coordonner la lutte contre la cybercriminalité.



**CNIL**  
Protéger la vie privée et les libertés individuelles ou publiques.



**CASES**  
Portail luxembourgeois de la sécurité de l'information



**Microsoft**  
Pour la sécurité et l'accompagnement des enfants dans

Retour