

Correctifs & Vulnérabilités

Impacts techniques

19 mai 2010

Sébastien RAILLARD
(COEXSI)

Faille DNS –2008

US-CERT : CVE-2008-1447/TA08-190B

The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."

Microsoft : MS08-037

Vulnerabilities in DNS could allow spoofing

Faille DNS –2008

Concernant les vulnérabilités DNS :

- Malheureusement récurrentes
- Souvent liées à l'authentification

Besoin :

Augmenter l'aléatoire pour limiter les risques

- Travail sur les identifiants de transaction
- Travail sur les algorithmes
- Travail sur les numéros de port utilisés

Faible DNS – 2008

Exemple Windows 2008 R2 :

- Publication du patch KB951746 pour le serveur DNS en juillet 2008

Impacts techniques :

- Passage de 1 port UDP en écoute à 2500 (!)
- Problèmes liés à l'utilisation des ressources
- Deux ans après, certaines applications natives ne sont toujours pas compatibles (WDS)
- Peu de discussion sur le sujet et peu d'information
- Diagnostique pouvant être couteux
- Pertinence dans le contexte domaine de petites et moyennes structures

Faille OpenSSL/Debian – 2008

- « Patch » généralement associé à Microsoft... pas toujours
- Faille découverte dans le PRNG de la librairie OpenSSL uniquement pour Debian et ses dérivés (Ubuntu...)
- La librairie OpenSSL est universellement utilisée (OpenSSH, OpenVPN, HTTPS,...)
- Présente presque 2 ans entre 2006 et 2008



Faille OpenSSL/Debian – 2008

Question : comment une telle régression a-t-elle pu apparaître lors de l'intégration d'une librairie dans une distribution linux ?

- **Librairie Intégrée = Librairie (Re)-Compilée**
- **Responsable de packages au sein des distributions**
- **Règles de réglages de la « sensibilité » du compilateur**
- **Génère beaucoup de « Warning », comme ces deux lignes :**
 - `MD_Update(&m,buf,j);`
 - `[..]`
 - `MD_Update(&m,buf,j); /* purify complains */`
- **Correction simple, on supprime ce qui gêne !**
- **Pas de chance, c'étaient les fonctions les plus critiques du PRNG...**

Faille OpenSSL/Debian – 2008

Impacts techniques :

- **Beaucoup de clefs générées sont « creuses »**
- **Migration vers des systèmes hors filiation Debian**
- **Période de vulnérabilité très longue (2 ans)**
- **Outils pour tester la sûreté des clefs générées :**
 - **Pas de garantie complète des tests**
 - **Difficulté à tester toutes les clefs**
- **Interrogations sur la chaîne d'intégration**

Correctifs Open-Source

Exemple de d'organisation :

- Une équipe développe un projet open-source
- Ce projet repose sur d'autres projets open-source (bibliothèques)
- Les autres projets peuvent être développées par des équipes différentes
- Ces projets sont intégrés dans des distributions type « linux » par encore d'autres équipes

Conclusion :

- Personnes différentes
- Ratio personnel/professionnel différent
- Pas de hiérarchie, pas de chaînes de responsabilité
- Modèles différents (GNU, mixte privé/communautaire, etc...)
- Cheminement complexe des patches

Correctifs Open-Source

Navigateur Firefox 3.5 avec Ubuntu 9.10 :

- Mise à jour effectuée via la distribution
- Bulletins de sécurité et versions peu lisibles :
 - Version: 3.5.9+nobinonly-0ubuntu0.9.10.1 2010-04-09 23:01:30 UTC
 - Version: 3.5.8+build1+nobinonly-0ubuntu0.9.10.1 2010-02-17 22:01:05 UTC
 - Version: 3.5.7+nobinonly-0ubuntu0.9.10.1 2010-01-08 01:01:27 UTC
 - Version: 3.5.6+nobinonly-0ubuntu0.9.10.1 2009-12-18 22:01:43 UTC
 - Version: 3.5.5+nobinonly-0ubuntu0.9.10.1 2009-11-11 17:00:57 UTC
 - Version: 3.5.4+nobinonly-0ubuntu0.9.10.1 2009-10-30 22:01:08 UTC

Méthodes de mise à jour :

- Parfois application des patches proposés
 - Parfois intégration d'une nouvelle version mineure
- => Risque d'évolution des fonctionnalités (ex: MySQL)

Correctifs Open-Source

Conclusion :

- Communauté Open-Source réactive mais pas sur tous les projets
- Communauté non organisée par définition
- Cheminement non déterministe des correctifs
- Pas de méthode unique de gestion des correctifs
- Risque d'impact fonctionnel