4INFOS8ProSec — Projets bibliographiques

Olivier Levillain

février-mars 2019

Pour l'évaluation de ce cours de programmation sécurisée, vous aurez à réaliser un projet bibliographique. Il comptera pour un tiers de votre note. Les objectifs de ce projet sont les suivants :

— chercher de l'information sur une faille ;
— présenter votre démarche de recherche ;
— expliquer la vulnérabilité et son impact ;
— analyser les réponses à apporter (court et long terme), sans se limiter aux modifications du code.

Afin de réaliser ce projet, vous travaillerez en binôme (idéalement, vous éviterez de travailler avec une personne de la promotion avec laquelle vous avez déjà réalisé un projet). Vous devrez préparer une soutenance qui aura lieu pendant un des créneaux d'avril prochain. Vous disposerez de 20 minutes pour la présentation devant la classe, qui sera suivie de 15 minutes de questions.

Concrètement, votre présentation devra comporter les éléments suivants :

— une brève description de votre démarche de recherche et de vos sources ;
— une présentation de la vulnérabilité et du logiciel affecté ;
— une description de la réponse proposée pour corriger (correctif, contournement proposés, etc.) ;
— (si possible) une frise chronologique donnant des éléments calendaires ;
— une analyse de l'impact concret dans des déploiements typiques ;
— des éléments d'analyse des causes sous-jacentes ;
— des propositions concrètes pour éviter qu'un tel problème se reproduise (dans le logiciel affecté ou un autre). Ces propositions peuvent toucher à la méthodologie de développement, à la chaîne de compilation ou sur des contraintes lors du déploiement ;
— (si vous avez le temps) une démonstration reproduisant le problème (soit avec une version vulnérable, soit avec un programme simplifié reproduisant le problème).

Pour la session de février-mars 2019, les sujets proposés sont les suivants :

— accès non autorisé à des fichiers privilégiés dans OpenSSH (CVE-2011-4327) [Système]
— biais RC4 pour décrypter une session TLS (`http://www.isg.rhul.ac.uk/tls/`) [Cryptographie]
— exécution arbitraire de code dans `tnftp` (CVE-2014-8517) [Réseau, langages]
— Faille Java « *Calendar* » (`http://blog.cr0.org/2009/05/write-once-own-everyone.html`, CVE-2008-5353) [Langages]
— Déréférencement de pointeur nul dans le noyau Linux (CVE-2009-2692, `http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html`) [Système, noyau]
— Oracle de *padding* dans SSH (`http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf`) [Crypto, sujet dur]
— SKIP-TLS (`https://www.mitls.org/pages/attacks/SMACK`) [Machine à états]
— BERserk NSS Signature Vulnerability (CVE-2014-1568) [Crypto, encodage, sujet dur]