2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport de défense n°D002]

SOMMAIRE

I. Description

N° d'attaque subie
Attaque n°2 sur notre serveur

Groupe ayant réalisé l'attaque
Groupe 2

- DEBUF-KAISER-JANATI-DEBRA (identifié grâce à l'adresse IP: 172.24.141.103)

Date de l'attaque
22/01/2014 entre 14h19 et 15h26

Catégorie d'attaque
Attaque automatisée (logiciel) sur notre application Web (WikiWikiWeb)

Technique utilisée
L'attaquant a émi un grand nombre de requête typique d'un logiciel d'attaque.

CID
L'application est restée accessible et aucune information n'a fuité.
Nous avons pu vérifier cette dernière affirmation en filtrant les requêtes réussies (HTTP Code 200) et en analysant leur contenu. Elles ne contenaient rien de particulier.

II. Dégâts subit

Description des dégâts

Les journaux montrent des URL avec des caractères encodées, du code SQL et des injections de chemins d'accès. Plus de 41 000 requêtes ont été émises en 1H.

Traces / Preuves laissées

Les requêtes ont bien été enregistrées par les logs de notre serveur (réussies et bloquées). Elles sont toutes disponibles dans les fichiers que nous avons joins à ce rapport.

III. Contre(s) mesure(s) mise(s) en place

L'attaque a partiellement était bloquée par nos modules Apache (mod_security et mod_evasive). Sur les 41 096 requêtes, seules 22 317 ont passé cette défense.

Ce résultat est globalement insuffisant, mais ces deux logiciels sont très difficiles à paramétrer.

Aucune mesure supplémentaire ne sera mise en oeuvre, nous devons encore implémenter celle de la première attaque.