

Vulnérabilités

Plusieurs dizaines de vulnérabilités sont publiées chaque jour mais peu d'entre elles sont réellement exploitées. L'impact de certaines vulnérabilités est parfois sous-estimé ou leurs conséquences mal appréhendées et de temps en temps l'application du correctif de sécurité adéquat ne suffit pas.

La faille OpenSSL spécifique à l'implémentation Debian et ses dérivées (Ubuntu) [1] a défrayé la chronique. Une modification très controversée dans le code OpenSSL spécifique à ces distributions a réduit drastiquement l'entropie du générateur aléatoire. Cette entropie se résumait alors à la valeur du PID courant (32768 valeurs possibles sur un Linux). L'impact de cette vulnérabilité était énorme et ne touchait pas uniquement les possesseurs de distributions Debian / Ubuntu mais toutes les applications se basant sur le matériel cryptographique généré par les versions d'OpenSSL vulnérables de ces distributions (du 17 septembre 2006 au 13 mai 2008...). Mettre à jour sa version d'OpenSSL était alors nécessaire pour ne plus se baser sur une cryptographie défaillante mais restait amplement insuffisant pour ne pas être victime des effets de cette vulnérabilité. En effet, tout le matériel cryptographique généré à partir des versions d'OpenSSL impactées pouvait être considéré comme compromis : clés asymétriques, certificats,

Références :

- [1] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166>,
- [2] <http://wiki.debian.org/SSLkeys>,
- [3] <http://www.metasploit.com/users/hdm/tools/debian-openssl/>,
- [4] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0450>,
- [5] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1860>.

etc [2]. Il est donc nécessaire de passer au peigne fin l'ensemble de ces équipements à la recherche des clés vulnérables pour les régénérer... ce qui est bien plus consommateur en temps que d'appliquer un simple correctif et surtout source d'oublis...

Il n'a pas fallu attendre bien longtemps avant de voir apparaître sur Internet les premières implémentations d'attaques, en particulier le brute-force de clés SSH [3]. En ayant préalablement calculé l'ensemble des couples de bi-clés pour les longueurs de clés courantes [3], une personne malveillante est en mesure de découvrir en quelques minutes la clé privée associée à un utilisateur donné s'authentifiant à l'aide d'une clé vulnérable. Les possibilités ne s'arrêtent pas là : il est possible de déchiffrer du trafic à posteriori, d'usurper l'identité d'un serveur, etc.

OpenSSL étant une bibliothèque très largement répandue, il n'est pas étonnant que les ramifications de cette vulnérabilité soient si importantes dès qu'elle touche les certificats générés : serveurs Web,

serveurs de messagerie, têtes de tunnel VPN, infrastructures de gestion de clés, etc.

On peut espérer que la forte médiatisation autour de cette vulnérabilité permettra une prise en compte la plus large possible... ce qui n'est pas forcément le cas avec certaines vulnérabilités, certes moins impressionnantes, mais dont les effets peuvent être dans certains cas tout aussi dévastateurs.

C'est le cas d'une vulnérabilité passée presque inaperçue touchant Apache/Tomcat [4] [5] et plus particulièrement le module de relayage mod_jk. Cette vulnérabilité de type *directory traversal* au travers d'un double encodage ("`..`" -> "`%252e%252e`" [%25 = "%", %2e = "."]) a exposé (et expose toujours...) des centaines d'interfaces d'administration Tomcat uniquement protégées par leur mot de passe d'administration, autant dire pas grand-chose quand dans la grande majorité des cas il s'agit des mots de passe par défaut. L'accès à cette interface permet alors de déployer trivialement un Webshell offrant une magnifique porte d'entrée pour la suite de l'intrusion. Cet exemple, loin d'être isolé, montre la difficulté d'appréciation relative à certaines failles jugées à tort peu ou moyennement critiques dans le milieu et qui s'avèrent pourtant très impactantes.

Ces deux exemples montrent bien que l'analyse des vulnérabilités n'est pas une tâche aisée et que dans certains cas la protection ne passe pas exclusivement par l'application du correctif de sécurité.



À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants - <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et s'intéresse de près à des sujets comme la sécurité des réseaux sans fils et la voix sur IP. Il a réalisé des interventions publiques sur ces sujets et a publié plusieurs articles, dont un article dans le numéro 14 de Hakin9 intitulé Sécurité Wi-Fi - WEP, WPA et WPA2. Il rédige un éditorial bimensuel dans Hakin9 depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr