ALERTE

Vulnérabilité d'OpenSSL 'Heartbleed' (CVE-2014-0160)

Première date de publication: 08 avril 2014

Les systèmes concernés

- OpenSSL 1.0.1 par 1.0.1f
- OpenSSL 1.0.2 - beta

Aperçu

Une vulnérabilité dans OpenSSL pourrait permettre à un attaquant distant d'exposer des données sensibles, y compris potentiellement des informations d'authentification des utilisateurs et les clés secrètes, à travers une manipulation incorrecte de la mémoire dans l'extension *heartbeat* de TLS.

Description

Les versions 1.0.1 à 1.0.1f d'OpenSSL contiennent une faille dans la mise en î uvre de la fonctionnalité heartbeat TLS/DTLS. Cette faille permet à un attaquant de récupérer la mémoire privée d'une application qui utilise la bibliothèque OpenSSL vulnérable en morceaux de 64k à la fois. Notez qu'un attaquant peut tirer profit de la vulnérabilité à plusieurs reprises pour récupérer autant de morceaux de 64k de mémoire qui sont nécessaires pour récupérer les secrets désirés. Les informations sensibles qui peuvent être récupérées à l'aide de cette vulnérabilité comprennent :

- Matériel de clé primaire (clés secrètes)
- Matériel de clé secondaire (noms d'utilisateur et mots de passe utilisés par les services vulnérables)
- Le contenu protégé (données sensibles utilisées par les services vulnérables)
- Informations collatérales (adresses de mémoire et de contenu qui peuvent être mis à profit pour contourner, exploiter les mesures d'atténuation)

Le code d'exploitation est disponible publiquement pour cette vulnérabilité. Des détails supplémentaires peuvent être trouvés dans CERT/CC Vulnerability Note VU#720951.

Impact

Cette faille permet à un attaquant distant de récupérer la mémoire privée d'une application qui utilise la bibliothèque OpenSSL vulnérable en morceaux de 64k à la fois.

Solution

OpenSSL 1.0.1g a été publié pour corriger cette vulnérabilité. Toutes les clés générées avec une version vulnérable de OpenSSL doivent être considérées comme compromises et régénérées puis déployées après que le patch ait été appliqué.

CIRT-BF recommande aux administrateurs système de considérer la mise en î uvre de Perfect Forward Secrecy pour atténuer les dommages qui pourraient être causés par la divulgation future de clés privées.

Références

- OpenSSL Security Advisory
- The Heartbleed Bug
- CERT/CC Vulnerability Note VU#720951
- Perfect Forward Secrecy
- RFC2409 Section 8 Perfect Forward Secrecy

Historique des révisions

- 08 avril 2014, première publication