Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 04 septembre 2017
N° CERTFR-2017-ACT-035

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-035

1 - Changement de clé DNSSEC

Le DNS (*Domain Name System*) est un protocole de diffusion de données dont le stockage est organisé à la façon d'une base de données répartie. La nature de ces données s'étend de la simple adresse IP à des politiques de filtrage des courriers électroniques, en passant par la distribution de matériel cryptographique.

DNSSEC, une extension de DNS, permet la signature cryptographique de ces données afin de garantir leur intégrité et leur authenticité, grâce à une infrastructure de gestion de clés (IGC) créée à cet effet. Contrairement à l'infrastructure de gestion de clés du Web (HTTPS), celle de DNSSEC ne possède qu'une seule racine de confiance ; une seule clé cryptographique qui permet ensuite de valider récursivement d'autres clés, et finalement les données contenues dans le DNS.

La clé servant actuellement de racine de confiance pour DNSSEC est entrée en production en juillet 2010, et elle est restée inchangée depuis lors. En 2016, une procédure a été amorcée par les administrateurs de la racine du DNS, l'ICANN et Verisign, afin de remplacer cette clé par une nouvelle. La nouvelle clé est de même nature et de même taille que la précédente : une clé RSA de longueur 2048 bits. Cette démarche est donc principalement engagée à des fins de tests de la procédure de renouvellement des clés. Elle permet aussi de limiter la période pendant laquelle un attaquant pourrait jouir de la compromission hypothétique de cette clé.

La nouvelle clé a été ajoutée à la racine du DNS en juillet 2017, et des signatures effectuées par cette clé seront publiées, en théorie, le 11 octobre 2017. Grâce au mécanisme détaillé par la RFC5011, et déjà implémenté et déployé dans la plupart des serveurs implémentant DNSSEC, aucune action n'est requise des administrateurs de ces serveurs. Ces derniers peuvent néanmoins consulter les journaux de leurs serveurs afin de s'assurer que la publication de la nouvelle clé racine a bien été prise en compte.

Pour les logiciels n'implémentant pas le mécanisme de la RFC5011, comme `systemd`, ou dans des cas particuliers, une opération *ad hoc* est nécessaire. Les administrateurs systèmes dont les serveurs valident les signatures DNSSEC sont invités à consulter la documentation de ces logiciels afin d'identifier la procédure à mettre en oeuvre.

Documentation

- RFC5011 :
  https://tools.ietf.org/html/rfc5011

2 - Rappel des avis émis

Dans la période du 28 août au 03 septembre 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-274 : Multiples vulnérabilités dans SCADA Schneider Electric PowerSCADA Expert

- CERTFR-2017-AVI-275 : Multiples vulnérabilités dans le noyau Linux d' Ubuntu
- CERTFR-2017-AVI-276 : Vulnérabilité dans MongoDB
- CERTFR-2017-AVI-277 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-278 : Multiples vulnérabilités dans Wireshark
- CERTFR-2017-AVI-279 : Multiples vulnérabilités dans les produits Siemens
- CERTFR-2017-AVI-280 : Multiples vulnérabilités dans PHP
- CERTFR-2017-AVI-281 : Multiples vulnérabilités dans Asterisk

Gestion détaillée du document

04 septembre 2017 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2017-ACT-035`