



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 12 septembre 2011
N° CERTA-2011-AVI-493-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Certificats SSL frauduleux

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-493>

Gestion du document

Référence	CERTA-2011-AVI-493-001
Titre	Certificats SSL frauduleux
Date de la première version	02 septembre 2011
Date de la dernière version	12 septembre 2011
Source	Billet de l'US-CERT du 30 août 2011
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Contournement de la politique de sécurité.

2 Systèmes affectés

Tous les systèmes utilisant des certificats SSL pour l'authentification, en particulier les navigateurs.

3 Résumé

Des certificats frauduleux ont été émis par une autorité de certification et peuvent servir à authentifier à tort des ordinateurs.

4 Description

Une vulnérabilité de l'autorité de certification (CA) DigiNotar a permis l'émission frauduleuse de certificats sur plusieurs domaines.

L'un de ces faux certificats a été utilisé pour monter une attaque trompant les internautes.

5 Solution

Certains éditeurs ont supprimé se la liste des certificats préinstallés dans leurs logiciels, ou simplement ou désactivé, le certificat de l'autorité DigiNotar.

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 2299 du 31 août 2011 :
<http://www.debian.org/security/2011/dsa-2299>
- Bulletin de sécurité Microsoft 2607712 du 29 août 2011 :
<http://www.microsoft.com/france/technet/security/advisory/2607712.mspx>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-34 du 30 août 2011 :
<http://www.mozilla.org/security/announce/2011/mfsa2011-34.html>
- Bulletin de sécurité Apple HT4920 du 09 septembre 2011 :
<http://support.apple.com/kb/HT4920>
- Bulletin du GOVCERT.NL du 31 août 2011 :
<http://www.govcert.nl/english/service-provision/knowledge-and-publication/factsheets/factsheet-fraudulent-issued-security-certificate-discovered.html>
- Billet de l'US-CERT du 30 août 2011 :
http://www.us-cert.gov/current/#fraudulent_diginotar_ssl_certificate

Gestion détaillée du document

02 septembre 2011 version initiale.

12 septembre 2011 ajout de la référence au bulletin de sécurité Apple.