

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-169>

Gestion du document

Référence	CERTA-2011-AVI-169
Titre	Certificats SSL frauduleux
Date de la première version	24 mars 2011
Date de la dernière version	–
Source(s)	Rapport d'incident de l'autorité de certification Comodo du 15 mars 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 sur un compte d'une autorité d'enregistrement (RA) affiliée à l'autorité de certification (CA) Comodo a permis l'émission frauduleuse de neuf certificats sur sept domaines différents.

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

5 Solution

Ces certificats sont mis en listes noires par certains logiciels.

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

6 Documentation

- Rapport d'incident de l'autorité de certification Comodo du 15 mars 2011 :
<http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>
- Bulletin de sécurité Debian 2011/dsa-2200 du 23 mars 2011 :
<http://www.debian.org/security/2011/dsa-2200>
- Bulletin de sécurité Google Chrome du 17 mars 2011 :
http://www.googlechromereleases.blogspot.com/2011/03/stable-and-beta-channel-updates_17.html
- Bulletin de sécurité Microsoft 2524375 du 23 mars 2011 :
<http://www.microsoft.com/france/technet/security/advisory/2524375.mspx>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-11 du 22 mars 2011 :
<http://www.mozilla.org/security/announce/2011/mfsa2011-11.html>

Gestion détaillée du document

24 mars 2011 version initiale.