



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 mai 2006
N° CERTA-2006-AVI-202

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du contrôle ActiveX i-Nav de Verisign

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-2006-AVI-202>

Gestion du document

Référence	CERTA-2006-AVI-202
Titre	Vulnérabilité du contrôle ActiveX I-Nav de Verisign
Date de la première version	17 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Zero Day Initiative
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Internet Explorer, Outlook et Outlook Express avec le greffon I-Nav de Verisign.

3 Résumé

Une mauvaise validation dans le contrôle ActiveX I-Nav permet à un utilisateur mal intentionné de faire exécuter du code arbitraire aux visiteurs d'un site web sous son contrôle.

4 Description

I-Nav est un contrôle ActiveX rajoutant le support des noms de domaines internationaux (IDN - « Internationalized Domain Names »). Ceci permet d'avoir des noms de domaines qui ne sont plus limités à l'ASCII 7 bits mais utilisant divers alphabets, et en particulier les caractères accentués dans le cas du français. Verisign a développé un greffon pour ajouter le support IDN à Internet Explorer, Outlook et Outlook Express.

Une absence de vérification dans une fonction du contrôle permet de faire exécuter du code arbitraire, dans le cas où l'utilisateur mal intentionné a réussi à emmener sa victime sur son site malveillant.

5 Solution

Se référer au site de l'éditeur pour l'obtention d'une version corrigée (cf. section Documentation).

6 Documentation

- Site internet de i-Nav :
<http://www.idnnow.com>
- Bulletin de sécurité Zero Day Initiative ZDI-06-014 :
<http://www.zerodayinitiative.com/advisories/ZDI-06-014.html>
- Référence CVE CVE-2006-2273 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2273>

Gestion détaillée du document

17 mai 2006 version initiale.