Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2002
N° CERTA-2002-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service d'accès Web *XWebMail* de la société XandMail

Gestion du document

Référence	CERTA-2002-AVI-062
Titre	Vulnérabilité dans le service d'accès Web *XWebMail* de la société XandMail
Date de la première version	26 mars 2002
Date de la dernière version	–
Source(s)	Société de services «Apogée Communications»
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

Accès au contenu d'une boîte aux lettres électronique et utilisation frauduleuse de celle-ci.

2 Systèmes affectés

Service d'accès au courrier électronique par le Web *XWebMail* de la société XandMail.

3 Résumé

Une vulnérabilité dans le service d'accès Web *XWebMail* de la société XandMail permet à un utilisateur mal intentionné d'accéder, sous certaines conditions, au compte d'un autre utilisateur, de lire et d'envoyer du courrier depuis ce compte.

4 Description

XWebMail est un service d'accès au courrier électronique via une interface Web.

Une vulnérabilité permet, dans certains cas, de trouver l'URL qui donne accès au compte d'un utilisateur, sans authentification préalable. Il est alors possible de lire le courrier de cet utilisateur et d'envoyer du courrier en son nom.

5 Solution

La société XandMail a affirmé au CERTA que tous les clients utilisant *XWebMail* étaient maintenant prévenus et que la vulnérabilité avait été corrigée, et le correctif livré de manière individuelle et personalisée.

Si vous offrez un service de messagerie par Web grâce au produit *XWebMail* et que vous n'avez pas été contacté par XandMail, envoyez un courrier électronique à l'adresse security@xandmail.com.

6 Remerciements

La vulnérabilité a été découverte par la société *Apogée Communications* (http://www.apogee-com.fr) durant un audit effectué auprès d'un de ses clients, qui utilisait *XWebMail*. Après avoir été alerté par *Apogée*, le CERTA a pu qualifier la vulnérabilité et contacter la société *XandMail*, dans le but d'élaborer une parade adéquate.

Gestion détaillée du document

26 mars 2002 version initiale.