

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Nortel Centrex IP CLient Manager

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-2005-AVI-412>

Gestion du document

Référence	CERTA-2005-AVI-412
Titre	Multiples vulnérabilités dans Nortel Centrex IP CLient Manager
Date de la première version	19 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Nortel #361442 du 14 octobre 2005
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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Nortel Centrex IP CLient Manager 2.5 ;
- Nortel Centrex IP CLient Manager 7.0 ;
- Nortel Centrex IP CLient Manager 8.0.

3 Description

Nortel vient de publier son bulletin de sécurité en réponse aux bulletins de sécurité de Microsoft du mois d'octobre.

Ces vulnérabilités ont été décrites dans les bulletins de sécurité du CERTA du 12 octobre 2005 :

- CERTA-2005-AVI-406 ;
- CERTA-2005-AVI-403 ;

- CERTA-2005-AVI-401 ;
- CERTA-2005-AVI-399 ;
- CERTA-2005-AVI-398 ;
- CERTA-2005-AVI-397 ;
- CERTA-2005-AVI-396 ;
- CERTA-2005-AVI-395 ;
- CERTA-2005-AVI-394.

4 Contournement provisoire

- Filtrer le trafic réseau à destination du système vulnérable ;
- ne pas naviguer sur des sites non sûrs.

5 Solution

Les mises à jours de sécurité seront disponibles lors de la prochaine publication de maintenance pour Centrex IP CLient Manager 2.5, 7.0 et 8.0.

6 Documentation

- Site Internet de l'éditeur :
<http://www.nortelnetworks.com/>
- Bulletin de sécurité Nortel #361442 du 14 octobre 2005 :
<http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=361442&RenditionID=>
- Bulletins de sécurité du CERTA :
<http://www.certa.ssi.gouv.fr/site/index.html#avis>

Gestion détaillée du document

19 octobre 2005 version initiale.