

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans EMC Legato Networker

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-2007-AVI-375>

Gestion du document

Référence	CERTA-2007-AVI-375
Titre	Vulnérabilité dans EMC Legato Networker
Date de la première version	23 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Zero Day Initiative ZDI-07-049 du 20 août 2007
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

– Networker versions 7.x.

3 Résumé

Une vulnérabilité de EMC Legato Networker permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité présente dans le service d'exécution à distance Networker Remote Exec Service permet à un utilisateur malveillant d'exécuter du code arbitraire à distance par le biais d'un dépassement de pile.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les clients de EMC peuvent se référer au bulletin de sécurité de l'éditeur présent dans sa base de connaissance sous la référence `esg83899`.

6 Documentation

- Base de connaissance de l'éditeur EMC :
<https://powerlink.emc.com>
- Bulletin de sécurité Zero Day Initiative ZDI-07-049 du 20 août 2007 :
<http://www.zerodayinitiative.com/advisories/ZDI-07-049.html>
- Référence CVE CVE-2007-3618 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3618>

Gestion détaillée du document

23 août 2007 version initiale.