

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans EMC Ionix

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-526>

Gestion du document

Référence	CERTA-2011-AVI-526
Titre	Vulnérabilité dans EMC Ionix
Date de la première version	20 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité EMC ESA-2011-029 du 14 septembre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Ionix Application Connectivity Monitor (Ionix ACM) version 2.3 et antérieures ;
- Ionix Adapter for Alcatel-Lucent 5620 SAM EMS (Ionix ASAM) version 3.2.0.2 et antérieures ;
- Ionix IP Management Suite (Ionix IP) version 8.1.1.1 et antérieures ;
- Ionix IPv6 Management Suite (Ionix IPv6) version 2.0.2 et antérieures ;
- Ionix MPLS Management Suite (Ionix MPLS) version 4.0.0 et antérieures ;
- Ionix Multicast Manager (Ionix MCAST) version 2.1 et antérieures ;
- Ionix Network Protocol Management Suite (Ionix NPM) version 3.1 et antérieures ;
- Ionix Optical Transport Management Suite (Ionix OTM) version 5.1 et antérieures ;
- Ionix Server Manager (EISM) version 3.0 et antérieures ;
- Ionix Service Assurance Management Suite (Ionix SAM) version 8.1.0.6 et antérieures ;
- Ionix Storage Insight for Availability Suite (Ionix SIA) version 2.3.1 et antérieures ;
- Ionix VoIP Availability Management Suite (Ionix VoIP AM) version 4.0.0.3 et antérieures ;

3 Résumé

Une vulnérabilité de type débordement de tampon peut être exploitée afin de provoquer un déni de service à distance et potentiellement une exécution de code arbitraire.

4 Description

Une vulnérabilité permet à une personne malintentionnée, en envoyant un paquet TCP ou UDP spécialement conçu, de provoquer un déni de service à distance ou potentiellement une exécution de code arbitraire.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité EMC ESA-2011-029 :
<http://archives.neohapsis.com/archives/bugtraq/2011-09/ESA-2011-029.txt>
- Référence CVE CVE-2011-2738 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2738>

Gestion détaillée du document

20 septembre 2011 version initiale.