Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2011
N° CERTA-2011-AVI-559

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Host Integration Server

Gestion du document

Référence	CERTA-2011-AVI-559
Titre	Vulnérabilités dans Microsoft Host Integration Server
Date de la première version	12 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-082 du 12 octobre 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

Déni de service à distance.

2 Systèmes affectés

- Microsoft Host Integration Server 2004 Service Pack 1 ;
- Microsoft Host Integration Server 2006 Service Pack 1 ;
- Microsoft Host Integration Server 2009 ;
- Microsoft Host Integration Server 2010.

/bin/bash: line 1: :wq: command not found
Deux vulnérabilités corrigées dans *Microsoft Host Integration Server* permettent à un attaquant de réaliser un déni de service au moyen de paquets TCP ou UDP spécialement conçus.

3 Description

Un utilisateur malveillant non authentifié peut provoquer un déni de service sur les programmes *snabase.exe*, *snaserver.exe*, *snalink.exe* et *mngagent.exe* en générant du traffic spécialement conçu sur les ports TCP 1477 et 1478, ou UDP 1478. Le déni de service est causé, soit par une boucle infinie (CVE-2011-2007), soit par un accès à de la mémoire non allouée (CVE-2011-2008).

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS11-082 du 12 octobre 2011 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS11-082
  http://technet.microsoft.com/en-us/security/bulletin/MS11-082
- Référence CVE CVE-2011-2007 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2007
- Référence CVE CVE-2011-2008 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2008

Gestion détaillée du document

12 octobre 2011 version initiale.