



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 novembre 2007
N° CERTA-2007-AVI-473

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les extensions de Nagios

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-473>

Gestion du document

Référence	CERTA-2007-AVI-473
Titre	Multiples vulnérabilités dans les extensions de Nagios
Date de la première version	02 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Fedora du 01 novembre 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

- Nagios Plugins versions 1.4.9 et antérieures (CVE-2007-5198) ;
- Nagios Plugins versions 1.4.10 et antérieures (CVE-2007-5623).

3 Résumé

Plusieurs vulnérabilités dans Nagios Plugins permettent à un utilisateur distant d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités sont présentes dans les extensions pour Nagios (Nagios Plugins) :

- la première est relative à l'extension *check_http* (CVE-2007-5198) et permet à un utilisateur distant d'exécuter du code arbitraire via un serveur web particulier si le paramètre *-f* a été passé à l'extension ;

- la seconde est relative à l'extension *check_snmp* (CVE-2007-5623) et permet à un utilisateur distant d'exécuter du code arbitraire via une réponse à une requête SNMP (*snmpget*) construite de façon particulière.

5 Solution

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

6 Documentation

- Site des extensions pour Nagios :
<http://nagiosplug.sourceforge.net/>
- Bulletin de sécurité Fedora du 01 novembre 2007 :
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00010.html>
- Bulletin de sécurité Ubuntu USN-532-1 du 02 novembre 2007 :
<http://www.ubuntulinux.org/usn/usn-532-1>
- Référence CVE CVE-2007-5623 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5623>
- Référence CVE CVE-2007-5198 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5198>

Gestion détaillée du document

02 novembre 2007 version initiale.