

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2011-AVI-414>

Gestion du document

Référence	CERTA-2011-AVI-414
Titre	Vulnérabilités dans Nagios
Date de la première version	27 juillet 2011
Date de la dernière version	–
Source	Site de téléchargement de Nagios
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

Injection de code indirecte à distance.

2 Systèmes affectés

Nagios, version 3.2.3 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans Nagios permettent de réaliser de l'injection de code indirecte (XSS).

4 Description

Plusieurs vulnérabilités sont présentes dans Nagios et permettent de réaliser de l'injection de code indirecte :

- un des paramètres en entrée de *config.cgi* est insuffisamment vérifié ;
- un des paramètres en entrée de *statusmap.cgi* est insuffisamment vérifié.

5 Solution

La version 3.3.1 de Nagios remédie à ces problèmes.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de téléchargement de Nagios :
<http://www.nagios.org/>
- Bulletin de sécurité Novell CVE-2011-1523 du 25 juillet 2011 :
<http://support.novell.com/security/cve/CVE-2011-1523.html>
- Bulletin de sécurité Novell CVE-2011-2179 du 25 juillet 2011 :
<http://support.novell.com/security/cve/CVE-2011-2179.html>
- Bulletin de sécurité Ubuntu USN-1151-1 du 15 juin 2011 :
<http://www.ubuntu.com/usn/usn-1151-1/>
- Référence CVE CVE-2011-1523 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1523>
- Référence CVE CVE-2011-2179 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2179>

Gestion détaillée du document

27 juillet 2011 version initiale.