

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans DotNetNuke

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-2008-AVI-460>

Gestion du document

Référence	CERTA-2008-AVI-460
Titre	Vulnérabilités dans DotNetNuke
Date de la première version	15 septembre 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité DotNetNuke 21, 22, 23
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

DotNetNuke versions antérieures à 4.9.0.

3 Résumé

De multiples vulnérabilités dans DotNetNuke permettent à une personne distante malintentionnée de porter atteinte à la confidentialité des données, d'élever ses privilèges et/ou de contourner la politique de sécurité.

4 Description

Trois vulnérabilités ont été corrigées dans DotNetNuke :

- une erreur dans la validation de l'identité des utilisateurs permet à une personne d'élever ses privilèges ;

- une erreur de validation dans le chargement de thèmes peut être exploitée pour contourner la politique de sécurité ;
- dans certaines circonstances il est possible de visionner la version du logiciel utilisé.

5 Solution

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

6 Documentation

- Site de téléchargement de DotNetNuke :
<http://www.dotnetnuke.com>
- Bulletin de sécurité DotNetNuke #21 du 09 septembre 2008 :
<http://www.dotnetnuke.com/News/SecurityPolicy/Securitybulletinno21/tabid/1174/Default.aspx>
- Bulletin de sécurité DotNetNuke #22 du 10 septembre 2008 :
<http://www.dotnetnuke.com/News/SecurityPolicy/Securitybulletinno22/tabid/1175/Default.aspx>
- Bulletin de sécurité DotNetNuke #23 du 10 septembre 2008 :
<http://www.dotnetnuke.com/News/SecurityPolicy/Securitybulletinno23/tabid/1176/Default.aspx>

Gestion détaillée du document

15 septembre 2008 version initiale.