

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service Gopher dans Microsoft Internet Explorer, Proxy Server et ISA Server

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-2002-AVI-128>

Gestion du document

Référence	CERTA-2002-AVI-128-001
Titre	Vulnérabilité du service gopher dans Microsoft Internet Explorer, Proxy Server et ISA Server
Date de la première version	13 juin 2002
Date de la dernière version	18 juin 2002
Source(s)	Bulletin de sécurité Microsoft #MS02-027
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 ;
- déni de service.

2 Systèmes affectés

- Microsoft Internet Explorer 5.01 SP2, 5.5 SP1, 5.5 SP2, 6.0 ;
- Microsoft Proxy Server 2.0 ;
- Microsoft ISA Server 2000.

3 Résumé

Un utilisateur mal intentionné peut effectuer un débordement de tampon et exécuter du code arbitraire sur la machine cible.

4 Description

Gopher est un protocole empirique utilisé pour la transmission de données de type texte sur l'Internet. Le protocole HTTP a rendu depuis obsolète son utilisation et l'on ne l'utilise plus que pour traiter les données qui n'ont pas encore été transférées vers HTTP. Les différents produits Microsoft permettent encore d'utiliser le protocole gopher dans un souci de compatibilité.

Microsoft Internet Explorer, Proxy Server et ISA Server utilisent la même fonction pour traiter le protocole gopher. Ils sont tous les trois vulnérables.

Un utilisateur mal intentionné peut utiliser cette vulnérabilité pour exécuter du code arbitraire sur l'ordinateur cible. Le code ainsi exécuté se verra appliquer les restrictions liées à l'utilisateur qui a démarré l'application.

- Pour Internet Explorer, les droits de l'utilisateur sont généralement limités ;
- Proxy Server et ISA Server fonctionnent généralement avec un haut niveau de privilèges permettant à un utilisateur mal intentionné de prendre le contrôle total du serveur.

5 Contournement provisoire

Il est possible de se protéger de cette attaque en configurant les différents produits de façon à ce qu'ils n'utilisent pas le protocole gopher :

- Pour Internet Explorer, configurer l'utilisation d'un serveur mandataire (proxy) pour le protocole gopher en faisant pointer l'adresse du serveur mandataire sur une machine ne traitant pas ce protocole (ex : localhost) ;
- pour ISA Server et Proxy Server, désactiver l'utilisation du protocole gopher.

Consulter le bulletin #MS02-027 de Microsoft pour avoir la procédure complète.

6 Solution

Des correctifs sont disponibles en téléchargement sur le site web de Microsoft.
<http://www.microsoft.com/technet/security/bulletin/MS02-027.asp>

7 Documentation

Bulletin de sécurité de Microsoft #MS02-027 :
<http://www.microsoft.com/technet/security/bulletin/MS02-027.asp>

Gestion détaillée du document

13 juin 2002 version initiale ;

18 juin 2002 deuxième version (révision de la section Solution).