

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GESTOR 2.21

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-063>

Gestion du document

Référence	CERTA-2002-AVI-063
Titre	Vulnérabilité dans GESTOR 2.21
Date de la première version	26 mars 2002
Date de la dernière version	–
Source(s)	
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

Publication de l'adresse IP de machines contenant des données nominatives.

2 Systèmes affectés

Gestor version 2.21.

3 Résumé

Gestor est un progiciel édité par la société GFI Progiciels.

Une fonction présente dans une bibliothèque javascript utilisée se connecte à plusieurs sites web pour délivrer des données à des fins de statistiques.

4 Description

Gestor est un progiciel destiné à la planification et à la gestion des temps (temps de travail par exemple). Il possède un module permettant d'effectuer des tâches d'administration et de consultation à distance au travers d'une

interface web. Ce module utilise une bibliothèque javascript (overhelp.js) librement distribuée par Erik Bosrup contenant une fonction de traçage mise en œuvre par un site de mesure d'audience (www.nedstat.nl). Cette fonction appelle trois URLs dont l'une contenant l'adresse IP du réseau local (adresse IP de la machine sur laquelle réside le module de consultation) et une référence à l'application gestor (obtenues au travers de la variable REFERER).

- <http://www.bosrup.com/web/overlib/o2/tr.gif>
- <http://www.nedstat.nl/cgi-bin/nedstat.gif?name=ol2t>
- http://www.nedstat.nl/cgi-bin/referstat.gif?name=ol2t&refer=http://x.x.x.x/gestor/formplanninga_u.asp
où X.X.X.X désigne l'adresse IP du serveur Gestor.

Aucune information nominative n'est toutefois transmise par ce procédé.

5 Contournement provisoire

Si l'application Gestor est sur une machine directement ou indirectement reliée à Internet, bloquer au niveau du pare-feu ou du relais HTTP l'adresse du serveur de statistiques (www.nedstat.nl) et du site d'Erik Bosrup (www.bosrup.com).

6 Solution

La société GFI a affirmé au CERTA que tous les clients utilisant Gestor version 2.21 étaient prévenus et que la vulnérabilité avait été corrigée sur leur plateforme. Contactez la société GFI si vous utilisez la version vulnérable du produit et que vous n'avez pas été contacté.

Gestion détaillée du document

26 mars 2002 version initiale.