



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 septembre 2002  
N° CERTA-2002-AVI-206

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité de mhonarc**

---

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-206>

---

### Gestion du document

Référence	CERTA-2002-AVI-206
Titre	Vulnérabilité de mhonarc
Date de la première version	13 septembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Debian DSA-163-1
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

- Usurpation d'identité ;
- Vol de cookies.

## 2 Systèmes affectés

Toutes les versions de mhonarc antérieures à la version 2.5.12.

## 3 Résumé

Une vulnérabilité dans mhonarc de type "cross site scripting" permet à un utilisateur mal intentionné de procéder à une usurpation d'identité.

## 4 Description

mhonarc est un utilitaire qui permet la conversion de fichiers de type message électronique au format HTML. En utilisant un message électronique contenant du HTML malicieusement construit, un utilisateur mal intentionné peut réaliser une usurpation d'identité et un vol de "cookies".

## 5 Contournement provisoire

Deux contournements provisoires sont possibles :

- Spécifier à `mhonarc` un fichier de ressources permettant l'exclusion des messages de type HTML. Les types MIME concernés sont : `text/html` et `text/x-html`. Pour ce faire, lancer `mhonarc` avec l'option `-rcfile <fichier.rc>`, où `<fichier.rc>` comprend les instructions suivantes :

```
<MIMEExcs>
text/html
text/x-html
</MIMEExcs>
```

- Spécifier à `mhonarc` un fichier de ressources permettant le traitement des messages de type HTML en les traitant comme du texte. Pour ce faire, lancer `mhonarc` avec l'option `-rcfile <fichier.rc>`, où `<fichier.rc>` comprend les instructions suivantes :

```
<MIMEFilters>
text/html; m2h_text_plain::filter; mhtxtplain.pl
text/x-html; m2h_text_plain::filter; mhtxtplain.pl
</MIMEFilters>
```

## 6 Solution

Installer la version 2.5.12.

## 7 Documentation

Avis de sécurité Debian DSA 163-1 :  
<http://www.debian.org/security/2002/dsa-163>

## Gestion détaillée du document

13 septembre 2002 version initiale.