



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 mars 2002  
N° CERTA-2002-AVI-065

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du logiciel Analog

---

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-065>

---

### Gestion du document

Référence	CERTA-2002-AVI-065
Titre	Vulnérabilité du logiciel Analog
Date de la première version	29 mars 2002
Date de la dernière version	–
Source(s)	Avis de Sécurité Debian DSA 125-1
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

- Exécution de code arbitraire ;
- récupération d'informations ;
- vol de cookies.

## 2 Systèmes affectés

Toutes les versions d'*Analog* antérieures à la version 5.22.

## 3 Résumé

*Analog* est vulnérable à une attaque de type « *cross-site scripting* ».

## 4 Description

*Analog* est un logiciel utilisé pour le traitement et l'analyse de logs d'un serveur HTTP. Il produit un rapport au format HTML.

Si un utilisateur mal intentionné envoie au serveur HTTP des requêtes contenant des chaînes de caractères, ces chaînes seront alors retranscrites dans les logs du serveur, puis dans le rapport *Analog*.

En choisissant judicieusement les chaînes à insérer (code Javascript par exemple), un utilisateur mal intentionné peut alors faire exécuter ce code par le navigateur de toute personne consultant le rapport créé par *Analog*.

## 5 Solution

Mettre à jour *Analog* en installant la version 5.22.

## 6 Documentation

- Avis de sécurité Debian DSA 125-1 :  
<http://www.debian.org/security/2002/dsa-125>
- Avis de sécurité Analog :  
<http://www.analog.cx/security4.html>
- Note d'information du CERTA sur le *cross-site scripting* :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

## Gestion détaillée du document

29 mars 2002 version initiale.