



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 7 avril 2003
N° CERTA-2003-AVI-026-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur le serveur Lotus Domino 6.0

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-2003-AVI-026>

Gestion du document

Référence	CERTA-2003-AVI-026-001
Titre	Vulnérabilités sur le serveur Lotus Domino 6.0
Date de la première version	20 février 2003
Date de la dernière version	7 avril 2003
Source(s)	NGSSoftware Insight Security Research
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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

- Le serveur Lotus Domino versions antérieures à la 5.0.12 et la version 6.0.
- Le composant iNotes du serveur Lotus Domino versions antérieures à la 5.0.12 et la version 6.0.

3 Résumé

Deux vulnérabilités ont été découvertes sur le serveur Lotus Domino et son composant iNotes qui permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le serveur Domino.

Une troisième vulnérabilité a été découverte dans le contrôle ActiveX nécessaire au composant iNotes installé sur les postes clients. Cette vulnérabilité permet d'exécuter du code arbitraire sur le poste client avec les privilèges de l'utilisateur.

4 Description

Le composant iNotes permet l'accès au serveur Lotus Domino via un navigateur Web ou d'autres clients que le client Lotus.

Deux vulnérabilités ont été découvertes sur le serveur Lotus Domino et son composant iNotes associé :

- Un débordement de pile est présent dans l'opération de redirection des URLs du serveur Lotus Domino. Un utilisateur mal intentionné peut, en utilisant une requête malicieusement construite, réaliser un déni de service ou exécuter du code arbitraire sur le serveur.
- Un second débordement de pile est présent dans le composant iNotes du serveur Lotus Domino. Une erreur dans le traitement du paramètre `PresetFields` permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le serveur avec les privilèges du serveur Lotus Domino.

Une troisième vulnérabilité a été découverte sur le contrôle ActiveX `LotusDominoSession` présent sur le poste client. L'envoi par message électronique ou par le protocole http d'une page html malicieusement construite permet d'exécuter du code arbitraire sur le système en utilisant les privilèges de l'utilisateur connecté.

5 Solution

Mettre à jour Lotus Domino avec la version 6.0.1 et le composant iNotes (cf. section documentation).

6 Documentation

- Mise à jour du composant iNotes :
http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-NOTECLNTi&S_TACT=&S_CMP=&sb=r
- Mise à jour de Lotus Domino :
http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTRSVRi&S_TACT=&S_CMP=&sb=r
- Avis de sécurité #NISR17022003a de NSGSoftware :
<http://www.securityfocus.com/archive/1/312043/2003-02-15/2003-02-21/0>
- Avis de sécurité #NISR17022003b de NSGSoftware :
<http://www.securityfocus.com/archive/1/312042/2003-02-15/2003-02-21/0>
- Avis de sécurité #NISR17022003c de NSGSoftware :
<http://www.securityfocus.com/archive/1/312047/2003-02-15/2003-02-21/0>

Gestion détaillée du document

20 février 2003 version initiale.

7 avril 2003 modification des versions des systèmes affectés.