Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mars 2011
N° CERTA-2011-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans syslog-ng

Gestion du document

Référence	CERTA-2011-AVI-132
Titre	Vulnérabilités dans syslog-ng
Date de la première version	04 mars 2011
Date de la dernière version	–
Sources	Annonces des versions de syslog-ng du 24 février 2011
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 à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

syslog-ng Premium Edition 3.0.x, 3.2.x et 4.0.x.

3 Résumé

Plusieurs vulnérabilités dans syslog-ng permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance ou de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités sont présentes dans syslog-ng Premium Edition :

- des débordements d'entiers dans la version utilisée de la bibliothèque GLib permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance ;

– des erreurs dans la version utilisée de la bibliothèque OpenSSL permettent à un utilisateur malveillant de contourner la politique de sécurité.

5 Solution

Les versions 3.0.7a, 3.2.1b et 4.0.1a de syslog-ng Premium Edition corrigent ces problèmes.
Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Annonces des versions de syslog-ng du 24 février 2011 :
https://lists.balabit.com/pipermail/syslog-ng-announce/2011-February/000107.html
https://lists.balabit.com/pipermail/syslog-ng-announce/2011-February/000108.html
https://lists.balabit.com/pipermail/syslog-ng-announce/2011-February/000111.html
– Référence CVE CVE-2008-4316 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4316
– Référence CVE CVE-2008-7270 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7270
– Référence CVE CVE-2009-3555 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
– Référence CVE CVE-2010-4180 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4180

Gestion détaillée du document

04 mars 2011 version initiale.