Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 janvier 2011
N° CERTA-2011-AVI-032

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans syslog-ng

Gestion du document

Référence	CERTA-2011-AVI-032
Titre	Vulnérabilités dans syslog-ng
Date de la première version	26 janvier 2011
Date de la dernière version	–
Source(s)	Annonces des versions de syslog-ng des 07, 14 et 16 janvier 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

syslog-ng Open Source Edition :
- versions 3.0.x antérieures à la version 3.0.10 ;
- versions 3.1.x antérieures à la version 3.1.4 ;
- versions 3.2.x antérieures à la version 3.2.2.

syslog-ng Premium Edition :
- versions 3.0.x antérieures à la version 3.0.6a ;
- versions 3.2.x antérieures à la version 3.2.1a.

3 Résumé

Plusieurs vulnérabilités sont présentes dans syslog-ng. Elles permettent de contourner la politique de sécurité ou de provoquer un déni de service à distance.

4 Description

Plusieurs vulnérabilités sont présentes dans syslog-ng.

L'une d'elles permet de contourner la politique de sécurité en raison d'un mauvais positionnement des droits d'accès sur des fichiers.

Les autres sont exploitables pour provoquer un déni de service à distance.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Annonces des versions de syslog-ng du 07 janvier 2011 :
  https://lists.balabit.com/pipermail/syslog-ng-announce/2011-January/000101.html
  https://lists.balabit.com/pipermail/syslog-ng-announce/2011-January/000102.html
- Annonces des versions de syslog-ng du 14 janvier 2011 :
  https://lists.balabit.com/pipermail/syslog-ng-announce/2011-January/000103.html
  https://lists.balabit.com/pipermail/syslog-ng-announce/2011-January/000104.html
- Annonces des versions de syslog-ng du 16 janvier 2011 :
  https://lists.balabit.com/pipermail/syslog-ng-announce/2011-January/000105.html
- Référence CVE CVE-2009-0590 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0590
- Référence CVE CVE-2009-2409 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409
- Référence CVE CVE-2009-3245 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3245
- Référence CVE CVE-2010-0433 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0433
- Référence CVE CVE-2010-0740 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0740
- Référence CVE CVE-2010-0742 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0742
- Référence CVE CVE-2010-3864 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3864
- Référence CVE CVE-2011-0343 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0343

Gestion détaillée du document

26 janvier 2011 version initiale.