



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2011
N° CERTA-2011-AVI-264

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans OpenSUSE Build Service

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-2011-AVI-264>

Gestion du document

Référence	CERTA-2011-AVI-264
Titre	Vulnérabilités dans OpenSUSE Build Service
Date de la première version	28 avril 2011
Date de la dernière version	–
Source	Annnonce de versions OpenSUSE du 02 mars 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

- Atteinte à l'intégrité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- OpenSUSE Build Service :
- versions web 2.1.x ;
 - API, versions 2.0.x et 2.1.x.

3 Résumé

Des vulnérabilités dans OpenSUSE Build Service permettent à un utilisateur malveillant de réaliser de l'injection de code indirecte et de modifier les informations.

4 Description

OpenSUSE Build Service est une plateforme de développement et de distribution de paquets logiciels. Plusieurs vulnérabilités affectent ce produit :

- (CVE-2011-0462) plusieurs vulnérabilités de type XSS affectent l'interface web ;
- (CVE-2011-0466) des défauts de l'API permettent à un utilisateur malveillant de modifier des projets ou des paquets logiciels sans disposer de droits en écriture légitimes.

5 Solution

Les versions 2.0.8 et 2.1.6 corrigent ces problèmes.

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

6 Documentation

- Annonce de versions OpenSUSE du 02 mars 2011 :
<http://news.opensuse.org/2011/03/02/build-service-team-releases-new-versions-fixing-security-problems/>
- Référence CVE CVE-2011-0462 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0462>
- Référence CVE CVE-2011-0466 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0466>

Gestion détaillée du document

28 avril 2011 version initiale.