

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Invision Power Board

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-2010-AVI-216>

Gestion du document

Référence	CERTA-2010-AVI-216
Titre	Multiples vulnérabilités dans Invision Power Board
Date de la première version	18 mai 2010
Date de la dernière version	–
Source(s)	Mises à jour de sécurité Invision Power Board du 14 mai 2010
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 la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Invision Power Board 3.x ;
- Invision Power Board 2.x.

3 Résumé

Plusieurs vulnérabilités découvertes dans Invision Power Board permettent à un utilisateur distant malveillant de porter atteinte à la confidentialité des données ou de réaliser une injection de code indirecte.

4 Description

Deux vulnérabilités corrigées dans Invision Power Board permette à une personne malintentionnée de réaliser une attaque par injection de code indirecte. Une troisième vulnérabilité permet à un utilisateur distant malveillant

de porter atteinte à la confidentialité des données en ayant accès à un répertoire d'images dont l'emplacement est connu au préalable.

5 Solution

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

6 Documentation

- Annonces de correctifs de sécurité d'Invision Power Board du 14 mai 2010 :
<http://community.invisionpower.com/topic/310713-ipboard-30x-security-patch-released/>
<http://community.invisionpower.com/topic/306221-ipboard-236-and-305-security-update/>
<http://community.invisionpower.com/topic/308032-ipboard-305-security-update/>

Gestion détaillée du document

18 mai 2010 version initiale.