Avis de vulnérabilité

ISEC-2012-02-v-1.0

Groupe LP
Backbuilder
Authentication bypass

Notre métier : préserver le vôtre.

WWW.INTRINSEC.COM
215 AV G. CLEMENCEAU 92024 NANTERRE ● TÉL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78
SAS AU CAPITAL DE 480 000 € ● SIREN 402 336 085 ● TVA FR 19 402 336 085 ● APE 721Z

AVIS ISEC-V2012-02-v-1.0

Éditeur : **Groupe LP**

Produit : **Backbuilder (version PHP)**

Titre : **Contournement d'authentification**

Identifiant Intrinsec : **ISEC-V2012-02-v-1.0**

Date de publication : **9 novembre 2012**

Date de dernière mise à jour : **9 novembre 2012**

Niveau de risque : **Très élevé**

Exploitable : **A distance**

Impact :

- Contournement d'une mesure de sécurité

Description :

Le mécanisme de validation de l'authentification des utilisateurs peut être contourné, permettant à un utilisateur malveillant d'accéder à n'importe fonctionnalité de l'application sans être authentifié.

Versions concernées :

Les versions 3.4 et 3.5 de Backbuilder sont concernées. La vulnérabilité a été corrigée dans les versions supérieures à 3.6.

Solutions :

Migrer vers la version 3.6 de la solution Backbuilder ou ajouter un appel à la fonction PHP « exit() » juste après la ligne 160 du fichier « admin/inc/init.inc.php ».

Références :

Aucune.

Crédit :

Vulnérabilité découverte par Thibaud Binétruy

Vulnérabilité divulguée en concertation avec l'éditeur

Historique :

2012-11-05: Découverte de la vulnérabilité

2012-11-09: Notification de l'éditeur

2012-11-23: Divulgation coordonnée avec l'éditeur

ADVISORY ISEC-V2012-02-v-1.0

Editor: **Groupe LP**

Product: **Backbuilder (PHP Version)**

Title: **Authentication bypass**

Intrinsec ID: **ISEC-V2012-02-v-1.0**

Publication date: **November 9th 2012**

Last update: **November 9th 2012**

Risk level: **Very High**

Exploitable: **Remotely**

Impact:

- Security function bypass

Description:

The authentication validation mechanism can be bypassed, allowing a malicious user to access every application's function without being authenticated.

Versions affected:

Backbuilder Version 3.4 and 3.5 are affected. The vulnerability is corrected in the 3.6 version.

Solutions:

Update to the 3.6 version or add an «exit()» function call after line 160 in the « admin/inc/init.inc.php » file.

References:

None.

Credits:

Vulnerability discovered by Thibaud Binétruy

Vulnerability disclosed in coordination with the constructor

History:

2012-11-05: Vulnerability discovery

2012-11-09: Editor notification

2012-11-23: Coordinated Vulnerability Disclosure