



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 octobre 2011  
N° CERTA-2011-AVI-608

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les produits D-Link

---

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-608>

---

### Gestion du document

Référence	CERTA-2011-AVI-608
Titre	Vulnérabilité dans les produits D-Link
Date de la première version	31 octobre 2011
Date de la dernière version	–
Source(s)	Avis JVN #72640744 du 28 octobre 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 ;
- déni de service à distance.

## 2 Systèmes affectés

- D-Link séries DES-3800 *firmwares* antérieures au R4.50B052 ;
- D-Link séries DWL-2100AP *firmwares* antérieures au 2.50RC548 ;
- D-Link séries DWL-3200AP *firmwares* antérieures au 2.55RC549.

## 3 Résumé

Une vulnérabilité présente sur les produits D-Link peut être utilisée par un utilisateur malveillant pour exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité de type débordement de tampon a été identifiée dans le serveur SSH de certains produits D-Link. Une personne malveillante peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance.

## 5 Solution

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

Une mise à jour du *firmware* permet de corriger cette vulnérabilité. Il est aussi possible de désactiver le serveur SSH dans certains produits, si celui-ci n'est pas utilisé.

## 6 Documentation

- Avis JVN #72640744 du 28 octobre 2011 :  
<http://jvn.jp/en/jp/JVN72640744/index.html>
- Avis D-Link DL-VU-2011-001 (en japonais) :  
[http://www.dlink-jp.com/page/sc/F/security\\_info20111028.html](http://www.dlink-jp.com/page/sc/F/security_info20111028.html)
- Référence CVE CVE-2011-3992 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3992>

## Gestion détaillée du document

**31 octobre 2011** version initiale.