

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans pcAnywhere

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-2012-AVI-032>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2012-AVI-032-001 |
| Titre | Vulnérabilités dans pcAnywhere |
| Date de la première version | 26 janvier 2012 |
| Date de la dernière version | 08 février 2012 |
| Source(s) | Bulletin de sécurité SYM12-002 du 24 janvier 2012 |
| 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 ;
- élévation de privilèges.

2 Systèmes affectés

- Symantec pcAnywhere versions 12.5.x ;
- IT Management Suite 7.0 pcAnywhere Solution versions 12.5.x ;
- IT Management Suite 7.1 pcAnywhere Solution versions 12.6.x.

3 Résumé

Des vulnérabilités dans Symantec pcAnywhere permettent d'exécuter du code arbitraire à distance et d'élever les privilèges.

4 Description

Des vulnérabilités ont été découvertes dans *Symantec pcAnywhere* :

- un mauvais filtrage des données transmises pendant la phase d'authentification auprès du service en écoute sur le port 5631/tcp permet une exécution de code arbitraire à distance (CVE-2011-3478) ;
- un utilisateur légitime du système peut écraser des fichiers déposés pendant l'installation pour élever ses privilèges (CVE-2011-3479) ;
- durant un session client-serveur valide, certaines entrées peuvent provoquer une violation d'accès mettant fin à la session distante mais laissant la session cliente ouverte. Ceci peut avoir pour conséquence de permettre des connexions non autorisées à la session cliente (CVE-2012-0290).

5 Solution

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

6 Documentation

- Bulletin de sécurité Symantec SYM12-002 du 26 janvier 2012 :
http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20120124_00
- Référence CVE CVE-2011-3478 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3478>
- Référence CVE CVE-2011-3479 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3479>
- Référence CVE CVE-2012-0290 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0290>

Gestion détaillée du document

26 janvier 2012 version initiale ;

08 février 2012 ajout du CVE CVE-2012-0290.