PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de maintenance DCSSI-2008/46-M01

ZoneCentral v3.1, build 540

Certificat de référence : DCSSI-2008/46

Paris, le 22 avril 2009,

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Références

a) Procédure MAI/P/01 Continuité de l'assurance
b) « ZoneCentral version 3.1 - Cible de Sécurité CC niveau EAL2+ », référence CSZC31, version 2, révision 6, Prim'X Technologies
c) « Rapport de certification DCSSI-2008/46 - ZoneCentral v3.1, build 533 », 18 décembre 2008, SGDN/DCSSI
d) « Continuité d'assurance - Rapport d'analyse d'impact - ZoneCentral v3.1 Build 540 » référence PX91158, version 1, révision 1, Prim'X Technologies

Identification du produit maintenu

Le produit maintenu est ZoneCentral v3.1, build 540 développé par Prim'X Technologies.

Description des évolutions

Les modifications du produit ZoneCentral v3.1 prises en compte ici concernent les corrections d'anomalies (bogues fonctionnels), et les améliorations et optimisations du produit suivantes :

- optimisation du nombre de zones chiffrées temporaires de l'Agent CryptUpdate ;
- accessibilité des commandes ShowPolicies et ExportPolicies dans l'outil zcucmd.exe ;
- activation du module X12 de ZoneCentral, fournisseur de services cryptographiques, même si les magasins CSP ne sont pas autorisés ;
- amélioration de la détection des clés USB ou des cartes à puce en mode PKCS#11 ;
- correction d'un problème de traitement des caractères accentués avec certains middlewares PKCS#11 ;
- correction liée à la notification à tort de changement des accès obligatoires ;
- correction du refus de chiffrement à tort d'un disque dur externe dans un cas particulier de configuration de politiques ;
- correction d'un problème de détection du dossier CSC (cache des fichiers offline) dans un cas de configuration système rare ;
- correction du refus de changement de clé dans une configuration particulière des politiques ;
- correction de l'échec du chiffrement dans une configuration Vista sans fichier de swap ;
- contournement d'un problème de compatibilité avec GemSafe 5.x en mode Pkcs#11 ;
- correction du chiffrement à tort de dossiers système dans un profil utilisateur Vista ;
- correction de l'échec de l'assistant de chiffrement sur expiration de mot de passe lorsque la liste d'accès personnelle était en lecture seule ;
- correction d'une demande inopportune d'ouverture de zone avant une mise en veille ;
- amélioration du traitement des erreurs dans la commande ZCACmd Defrag, commande technique permettant de réunir les zones chiffrées identiques et redondantes dans une arborescence ;
- message d'erreur inopportun lors du lancement de CryptUpdate quand aucun certificat valide n'était trouvé ;
- optimisation du délai de l'arrêt système quand l'effacement du swap à l'arrêt du système et le chiffrement du swap par ZoneCentral sont activés ;
- amélioration du démontage des clés USB utilisées comme porte-clés ;
- surgénération inutile d'un type d'événements dans les fichiers de log ;
- correction d'un trap aléatoire ;
- correction d'un trap explorer ;
- correction du défaut d'affichage d'un avertissement avec la politique P189 ;

- amélioration d'un message d'erreur peu ergonomique lorsque le domaine n'est pas joignable ;
- correction de l'échec de recherche de certificats avec un « common name » contenant le caractère '\' ;
- échec d'accès à un partage DFS sous Vista ;
- échec d'appel PKCS#11 C_GetAttributeValue qui empêchait l'utilisation de certaines cartes à puce ;
- ajout d'une politique de désactivation de l'image de fond de dossier dans l'explorateur ;
- correction du chiffrement à tort des disques durs amovibles quand la consigne de chiffrement est positionnée à « tous les disques locaux » ;
- amélioration des performances d'affichage des icônes ZoneCentral dans l'explorateur Windows ;
- création automatique d'un dossier si le dossier indiqué dans la politique P343 n'est pas renseigné ;
- correction du blocage du poste sur les portables Toshiba équipés d'un capteur d'empreinte digitale ;
- correction du blocage du poste quand le produit FortiClient est installé avec ZoneCentral ;
- correction de l'affichage à tort des fichiers de contrôle sur les racines de partage réseau ;
- correction du refus de masterisation multiple.

Le détail de ces modifications est disponible sur le site web du développeur www.primx.eu

Fournitures impactées

Les fournitures d'évaluation impactées sont le code source du produit et sa liste de configuration.
Par rapport aux références documentaires identifiées dans le certificat initial (référence c, annexe 2), seul le document suivant a évolué :

[CONF]	« Liste de configuration ZoneCentral 3.1 build 540 », référence PX81112, version 1, révision 4, Prim'X Technologies

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.
Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.

Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, la République de Corée, le Pakistan, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.