



Communiqué de presse

Fortinet lance un nouvel outil de protection contre l'attaque « Curse of Silence/CurseSMS » qui vise les téléphones mobiles

L'outil FortiCleanUp de Fortinet permet de rétablir le bon fonctionnement des téléphones mobiles attaqués

Paris, le 7 janvier 2009 - Fortinet®, pionnier et leader de solutions de gestion unifiée des menaces (unified threat management : UTM), a annoncé aujourd'hui que son équipe de recherche en sécurité FortiGuard®, a publié une nouvelle version du FortiCleanUp, permettant aux utilisateurs de rétablir le bon fonctionnement des téléphones mobiles touchés par l'attaque « Curse of Silence » (aussi connu sous le nom de « CurseSMS »). FortiCleanUp est un outil gratuit fonctionnant sur les téléphones mobiles équipés du système d'exploitation Symbian™OS S60. Il a été conçu spécifiquement pour protéger les téléphones mobiles contre des attaques spécifiques telles « Curse of Silence ».

« Curse of silence » est une attaque à distance du type déni de service, qui se propage par les SMS et les MMS. Elle a été découverte récemment par Tobias Engel et révélée au public à l'occasion du 25^{ème} « Chaos Communication Congress ». L'attaque consiste à envoyer un SMS comportant une commande malicieuse à des cibles potentielles. Dès la réception de ce SMS, le téléphone pris pour cible risque de ne plus pouvoir recevoir de messages SMS ou MMS. Selon la version du système d'exploitation dont est équipé le téléphone mobile attaqué, il peut être nécessaire de revenir à la configuration d'origine pour que le téléphone fonctionne à nouveau.

Fortinet propose une licence gratuite de son outil FortiCleanUp, qui permet à l'utilisateur de rétablir le fonctionnement du téléphone portable qui a été attaqué. La version du FortiCleanUp conçu pour contrer l'attaque « Curse of Silence » analyse automatiquement les messages SMS et MMS, puis supprime les « faux » SMS ou MMS qui empêchent le bon fonctionnement du téléphone.

Parmi les modèles potentiellement vulnérables, on compte les téléphones Nokia équipés du système d'exploitation SymbianOS S60 2ème édition du Feature Pack 2, 2ème édition du Feature Pack 3, 3ème édition, et 3ème édition du Feature Pack 1. Plusieurs téléphones de la série « N » (jusqu'au modèle N95) et de la série « E » (jusqu'au modèle E90), ainsi que des modèles plus anciens, tels que le 6680, sont concernés.

Pour une protection complète en temps réel, l'équipe FortiGuard recommande aux utilisateurs d'installer sur leur téléphone portable l'anti-virus FortiClient Mobile développé par Fortinet. Cette application de sécurité propose les fonctionnalités d'un système de sécurité unifié comprenant un pare-feu personnel, un RPV IPSec, un anti-virus, un anti-spyware et un anti-spam SMS. Le système de protection FortiClient a été conçu par les équipes des services de sécurité FortiGuard de Fortinet, dans le but de favoriser la protection des téléphones contre toutes les sortes de menaces actuelles. FortiClient Mobile est une application qui permet de bénéficier des fonctionnalités d'un système de sécurité unifié. Elle est disponible pour les systèmes d'exploitation Microsoft® Windows Mobile™ et SymbianOS S60.

Des informations détaillées sur l'attaque "Curse of Silence" et la liste complète des téléphones Nokia concernés sont disponibles sur: <http://www.fortiguardscenter.com/advisory/FGA-2008-31.html>.

Pour plus d'informations sur les recherches de l'équipe FortiGuard connectez vous sur (<http://www.fortiguardscenter.com/>) ou ajoutez le lien RSS <http://www.fortinet.com/FortiGuardCenter/rss/index.html>. Pour en savoir plus sur le service FortiGuard : <http://www.fortinet.com/products/fortiguard.html>.

À propos de Fortinet

Fortinet est le précurseur et le leader des systèmes unifiés de sécurité UTM (*Unified Threat Management*) basés sur des accélérateurs de performance ASIC et utilisés par les entreprises et service providers pour garantir leur sécurité tout en réduisant leurs coûts d'exploitation. Les solutions Fortinet constituent la nouvelle génération des systèmes de protection de réseau en temps réel et ont été conçues pour intégrer plusieurs niveaux de sécurité – incluant les fonctions pare-feu, antivirus, antispam, VPN, filtrage de contenu, et prévention des intrusions et spyware– permettant à ses clients de détecter et de contrer en temps réel les attaques faites au niveau du réseau et du contenu. Basées sur la technologie ASIC et sur une interface unifiée, les solutions Fortinet offrent des fonctionnalités avancées en matière de sécurité, qui s'étendent de l'utilisateur nomade aux installations basées sur châssis intégrant gestion et reporting.

Les solutions Fortinet ont reçu de nombreuses récompenses à travers le monde et sont les seuls produits de sécurité à détenir six certifications ICSA Labs (pare-feu, antivirus, IPSec, SSL, IPS réseau et antispam). Fortinet est une société privée dont le siège Europe Afrique Moyen-Orient se situe à Sophia Antipolis, en France.

#

Copyright © 2009 Fortinet, Inc. Tous droits réservés. Les symboles ® et ™ sont déposés et non enregistrée par la marque IncFortinet, qui est une marque commerciale déposée de Fortinet, Inc. Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiDB, APSecure, et ABACAS. sont des marques commerciales de Fortinet, Inc. aux États-Unis et/ou dans d'autres pays du monde. L'ensemble des marques commerciales citées dans le présent communiqué sont la propriété de leurs détenteurs respectifs.

Point Virgule Relations Presse

Elodie Repellin – Sandra Labérenne
9, avenue de Clichy – 75017 Paris
Tél. : 01 73 79 50 64 – 01 73 79 50 68
Email : erepellin@pvirgule.fr /
slaberenne@pvirgule.fr
Site internet : www.pointvirgule.fr

Fortinet

Barbara Maignet
Responsable Relations Presse EMEA
Tél. : 04 89 87 05 52
Email : bmaigret@fortinet.com
Site internet : www.fortinet.com