Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 30 novembre 2015
N° CERTFR-2015-ACT-048

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-048

1 - eDellRoot

Au début de l'année 2015, le fabricant d'ordinateurs portables chinois Lenovo avait fait les titres de l'actualité de la sécurité informatique. En effet, les ordinateurs du constructeur étaient livrés avec le logiciel Superfish et une autorité de certification associée qui permettaient d'injecter des publicités au sein des pages de réponse du moteur de recherche Google.

De façon similaire, le constructeur Dell a fait l'objet d'un papier publié par des chercheurs en sécurité présentant leurs découvertes. Récemment, les ordinateurs Dell étaient livrés avec deux certificats pré-installés qui ne correspondent pas à des autorités de certification traditionnelles. Le premier d'entre eux, appelé eDellRoot, est fourni avec la clé privée correspondante. Bien qu'ayant été installé avec l'attribut non exportable, il est possible de l'extraire à l'aide d'outils spécifiques. À titre de référence, ce certificat, déployé lors de l'installation de l'application Dell Foundation Services, possède l'empreinte SHA1 suivante : 98:A0:4E:41:63:35:77:90:C4:A7:9E:6D:71:3F:F0:AF:51:FE:69:27.

Tout utilisateur d'un ordinateur Dell ayant le certificat racine eDellRoot reconnaît comme valide un certificat signé à l'aide de la clé privée de celui-ci. Un attaquant en possession de cette clé serait donc capable de mettre en place une attaque dite de l'homme du milieu, permettant de rediriger le trafic réseau vers un serveur sous son contrôle et de déchiffrer les flux sécurisés, sans éveiller les soupçons de sa victime. Une seconde découverte concerne les pilotes Atheros pour les outils de gestion de périphériques Bluetooth. Une archive Verisign.pfx protégée par un mot de passe faible comporte également la clé privée permettant de signer des pilotes illégitimes. Cependant, ce certificat est expiré depuis le 31 mars 2013 et n'est par conséquent plus reconnu comme étant de confiance.

Le CERT-FR recommande l'application de la procédure de suppression du certificat eDellRoot ainsi que l'installation du correctif pour l'application Dell Foundation Services publié par Dell. D'autre part, le CERT-FR recommande, lors de l'acquisition de nouveau matériel, de procéder à la réinstallation du système d'exploitation ou de supprimer les applications tierces fournies par le fabricant lorsqu'elles ne sont pas nécessaires au bon fonctionnement et à la gestion de l'ordinateur.

Documentation

- https://www.duosecurity.com/static/pdf/Dude,_You_Got_Dell_d.pdf
- https://dellupdater.dell.com/Downloads/APP009/eDellRootCertificateRemovalInstructions.pdf
- https://dellupdater.dell.com/Downloads/APP009/eDellRootCertFix.exe

2 - Les risques associés au déverrouillage d'un ordiphone

Dès l'apparition des premiers ordiphones sur le marché, des moyens ont été recherchés pour effectuer des modifications sur le système d'exploitation embarqué et ce, pour plusieurs raisons :

- historiquement, l'utilisation d'un terminal avec le réseau téléphonique d'un autre opérateur. Certaines gammes de terminaux étant bloquées pour ne fonctionner qu'avec l'opérateur signant un contrat d'exclusivité avec le constructeur (AT&T et Apple aux Etats-Unis, par exemple) ;

– l'installation d'applications depuis un magasin tiers, en général pour éviter de payer l'application disponible sur le magasin officiel ;
– éviter à un développeur de devoir soumettre son application à l'approbation et au respect des conditions d'utilisation du magasin officiel ;
– modifier l'apparence du terminal : thèmes, icônes, frimousses ;
– dans certains cas, procéder à l'investigation numérique d'un appareil en acquérant une image du système.

Or, les opérations de déverrouillage (qui ne doivent pas être confondu avec le déverrouillage du téléphone pour utiliser la SIM d'un autre opérateur) modifient le niveau de sécurité du téléphone :

– l'installation d'une ROM modifiée, si elle est mal effectuée, peut bloquer le téléphone *(bricking)* ;
– le déverrouillage permet principalement d'augmenter les privilèges de l'utilisateur, passant outre le modèle de sécurité basé sur les restrictions imposées à l'utilisateur et aux privilèges accordés aux applications qu'il lance ;
– le procédé de déverrouillage active automatiquement certains services comme SSH sur iPhone, dont le mot de passe fût un temps identique sur tous les terminaux ;
– l'installation d'applications non signées depuis un magasin tiers augmente le risque d'installation d'applications illégitimes ou vérolées (ver, vol d'information, publicité).

Les techniques de déverrouillage d'un ordiphone offrent des possibilités pour les développeurs et les experts en sécurité de mieux étudier le fonctionnement du système embarqué. En revanche elles ne doivent pas être employées sur des terminaux destinés à des utilisateurs finaux, au risque de les exposer à des risques de piratage ou d'infection virale.

Pour ces raisons, le CERT-FR recommande d'éviter le déverrouillage d'un ordiphone issu d'une flotte gérée par une entreprise ou une administration et de limiter cette technique à un environnement de test, sans données personnelles ou professionnelles.

3 - Rappel des avis émis

Dans la période du 23 au 29 novembre 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-AVI-497 : Vulnérabilité dans Wireshark
– CERTFR-2015-AVI-498 : Multiples vulnérabilités dans les noyaux Linux Red Hat
– CERTFR-2015-AVI-499 : Vulnérabilité dans Cisco TelePresence Video Communication Server
– CERTFR-2015-AVI-500 : Vulnérabilité dans Cisco Networking Services
– CERTFR-2015-AVI-501 : Vulnérabilité dans Cisco Virtual Topology System
– CERTFR-2015-AVI-502 : Vulnérabilité dans Cisco Firepower 9000 Series Switch
– CERTFR-2015-AVI-503 : Vulnérabilité dans Cisco ASA
– CERTFR-2015-AVI-504 : Vulnérabilité dans Blue Coat Unified Agent
– CERTFR-2015-AVI-505 : Vulnérabilité dans les produits Cisco
– CERTFR-2015-AVI-506 : Vulnérabilité dans Cisco ASR 5000
– CERTFR-2015-AVI-507 : Vulnérabilité dans Xen

Gestion détaillée du document

30 novembre 2015 version initiale.