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 22 décembre 2015
N° CERTFR-2015-ALE-009-1

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Apple Mac OS X

Gestion du document

Référence	CERTFR-2015-ALE-009
Titre	Vulnérabilité dans Apple Mac OS X
Date de la première version	24 juillet 2015
Date de la dernière version	22 décembre 2015
Source(s)	OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability
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(s)

– élévation de privilèges

2 - Systèmes affectés

Mac OS X versions 10.10.0 à 10.10.4

3 - Résumé

Une vulnérabilité a été découverte dans *Apple Mac OS X*. Elle permet à un attaquant de provoquer une élévation de privilèges.

4 - Solution

L'exploitation de cette vulnérabilité se base sur la surcharge d'une variable d'environnement dans Mac OS 10.10.x. En effet, la variable d'environnement incriminée permet d'indiquer au système un fichier dans lequel journaliser des erreurs.

L'exploitation de cette vulnérabilité permet donc une écriture arbitraire de fichier avec des privilèges élevés et peut donc conduire à une élévation de privilèges.

Cette fonctionnalité n'est disponible qu'à partir de la version 10.10 de Mac OS X, les versions inférieures ne sont donc pas concernées.

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

5 - Documentation

- Bulletin de sécurité de l'éditeur
  https://support.apple.com/en-us/HT205031
- http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-355/index.html
- OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability
  https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html
- Extension de noyau SUIDGuard
  https://github.com/sektioneins/SUIDGuard

Gestion détaillée du document

24 juillet 2015 version initiale.
22 décembre 2015 clôture de l'alerte.