

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits Apple**

### Gestion du document

Référence	CERTFR-2017-AVI-028
Titre	Multiples vulnérabilités dans les produits Apple
Date de la première version	24 janvier 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT207482 du 23 janvier 2017 Bulletin de sécurité Apple HT207484 du 23 janvier 2017 Bulletin de sécurité Apple HT207483 du 23 janvier 2017 Bulletin de sécurité Apple HT207481 du 23 janvier 2017 Bulletin de sécurité Apple HT207486 du 23 janvier 2017 Bulletin de sécurité Apple HT207485 du 23 janvier 2017 Bulletin de sécurité Apple HT207487 du 23 janvier 2017
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)

- exécution de code arbitraire à distance
- déni de service
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

## 2 - Systèmes affectés

- iOS versions antérieures à 10.2.1
- Safari versions antérieures à 10.0.3
- macOS Sierra versions antérieures à 10.12.3
- iCloud pour Windows versions antérieures à 6.1.1
- iTunes pour Windows versions antérieures à 12.5.5
- tvOS versions antérieures à 10.1.1
- watchOS versions antérieures à 3.1.3

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Apple*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service et un contournement de la politique de sécurité.

### 4 - Solution

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

### 5 - Documentation

- Bulletin de sécurité Apple HT207482 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207482>
- Bulletin de sécurité Apple HT207484 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207484>
- Bulletin de sécurité Apple HT207483 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207483>
- Bulletin de sécurité Apple HT207481 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207481>
- Bulletin de sécurité Apple HT207486 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207486>
- Bulletin de sécurité Apple HT207485 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207485>
- Bulletin de sécurité Apple HT207487 du 23 janvier 2017  
<https://support.apple.com/en-us/HT207487>
- Référence CVE CVE-2016-1248  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1248>
- Référence CVE CVE-2016-4688  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4688>
- Référence CVE CVE-2016-4691  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4691>
- Référence CVE CVE-2016-4693  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4693>
- Référence CVE CVE-2016-7588  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7588>
- Référence CVE CVE-2016-7589  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7589>
- Référence CVE CVE-2016-7591  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7591>
- Référence CVE CVE-2016-7594  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7594>
- Référence CVE CVE-2016-7595  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7595>
- Référence CVE CVE-2016-7606  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7606>
- Référence CVE CVE-2016-7607  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7607>
- Référence CVE CVE-2016-7612  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7612>
- Référence CVE CVE-2016-7615  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7615>
- Référence CVE CVE-2016-7616  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7616>

- Référence CVE CVE-2016-7619  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7619>
- Référence CVE CVE-2016-7621  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7621>
- Référence CVE CVE-2016-7626  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7626>
- Référence CVE CVE-2016-7627  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7627>
- Référence CVE CVE-2016-7636  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7636>
- Référence CVE CVE-2016-7637  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7637>
- Référence CVE CVE-2016-7643  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7643>
- Référence CVE CVE-2016-7644  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7644>
- Référence CVE CVE-2016-7651  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7651>
- Référence CVE CVE-2016-7657  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7657>
- Référence CVE CVE-2016-7658  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7658>
- Référence CVE CVE-2016-7659  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7659>
- Référence CVE CVE-2016-7660  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7660>
- Référence CVE CVE-2016-7662  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7662>
- Référence CVE CVE-2016-7663  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7663>
- Référence CVE CVE-2016-8670  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8670>
- Référence CVE CVE-2016-8687  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8687>
- Référence CVE CVE-2016-9933  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9933>
- Référence CVE CVE-2016-9934  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9934>
- Référence CVE CVE-2017-2350  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2350>
- Référence CVE CVE-2017-2351  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2351>
- Référence CVE CVE-2017-2352  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2352>
- Référence CVE CVE-2017-2353  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2353>
- Référence CVE CVE-2017-2354  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2354>
- Référence CVE CVE-2017-2355  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2355>
- Référence CVE CVE-2017-2356  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2356>
- Référence CVE CVE-2017-2357  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2357>

- Référence CVE CVE-2017-2358  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2358>
- Référence CVE CVE-2017-2359  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2359>
- Référence CVE CVE-2017-2360  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2360>
- Référence CVE CVE-2017-2361  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2361>
- Référence CVE CVE-2017-2362  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2362>
- Référence CVE CVE-2017-2363  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2363>
- Référence CVE CVE-2017-2364  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2364>
- Référence CVE CVE-2017-2365  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2365>
- Référence CVE CVE-2017-2366  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2366>
- Référence CVE CVE-2017-2368  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2368>
- Référence CVE CVE-2017-2369  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2369>
- Référence CVE CVE-2017-2370  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2370>
- Référence CVE CVE-2017-2371  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2371>
- Référence CVE CVE-2017-2373  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2373>

## Gestion détaillée du document

**24 janvier 2017** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-028>

---