



CERT-In Advisory CIAD-2016-0078

Multiple Vulnerabilities in Apple iOS

Original Issue Date: December 14, 2016

Severity Rating: High

Software Affected

- Apple iOS prior to version 10.2

Overview

Multiple vulnerabilities have been reported in Apple iOS which could allow a remote attacker to execute arbitrary code, disclose sensitive information, bypass security controls, overwrite existing files, determine kernel memory layout, obtain contents of process memory, conduct universal cross site scripting attacks, execute arbitrary code with kernel privileges or cause denial of service conditions on the targeted system.

Description

These vulnerabilities exist due to issues in Accessibility, Accounts, Audio, CoreFoundation, CoreGraphics, CoreMedia External Displays, CoreMedia Playback, CoreText, Disk Images, Find My iPhone, FontParser, Graphics, Driver, ICU, Image Capture, ImageIO, IOHIDFamily, IOKit, Kernel, libarchive, Local Authentication, Mail, Media Player, Power Management, Profiles, Safari Reader, Security, SpringBoard, syslog, WebKit components of Apple iOS.

Successful exploitation of these vulnerabilities could allow a remote attacker to disclose sensitive information, bypass security controls, access restricted files, determine kernel memory layout, obtain contents of process memory, take advantage of cryptographically weak 3DES algorithm, execute arbitrary code with kernel privileges or cause denial of service conditions on the affected systems.

Solution

Apply appropriate security updates as mentioned in the [Apple Security Advisory HT207422](#)

Vendor Information

Apple

<https://support.apple.com/en-us/HT207422>

References

Security Tracker

<http://securitytracker.com/id/1037429>

CVE Name

[CVE-2016-7634](#)
[CVE-2016-7664](#)
[CVE-2016-7651](#)
[CVE-2016-7658](#)
[CVE-2016-7659](#)
[CVE-2016-7663](#)
[CVE-2016-7627](#)
[CVE-2016-7655](#)
[CVE-2016-7588](#)
[CVE-2016-7595](#)
[CVE-2016-7616](#)
[CVE-2016-7638](#)
[CVE-2016-4691](#)
[CVE-2016-4688](#)
[CVE-2016-7655](#)
[CVE-2016-7594](#)
[CVE-2016-4690](#)
[CVE-2016-7643](#)
[CVE-2016-7591](#)
[CVE-2016-7657](#)
[CVE-2016-7606](#)
[CVE-2016-7612](#)
[CVE-2016-7607](#)
[CVE-2016-7615](#)
[CVE-2016-7621](#)
[CVE-2016-7637](#)
[CVE-2016-7644](#)
[CVE-2016-7619](#)
[CVE-2016-7601](#)

- [CVE-2016-4689](#)
- [CVE-2016-7653](#)
- [CVE-2016-7661](#)
- [CVE-2016-7626](#)
- [CVE-2016-7650](#)
- [CVE-2016-4693](#)
- [CVE-2016-7636](#)
- [CVE-2016-7662](#)
- [CVE-2016-4781](#)
- [CVE-2016-7597](#)
- [CVE-2016-7660](#)
- [CVE-2016-4692](#)
- [CVE-2016-7635](#)
- [CVE-2016-7652](#)
- [CVE-2016-4743](#)
- [CVE-2016-7856](#)
- [CVE-2016-7587](#)
- [CVE-2016-7610](#)
- [CVE-2016-7611](#)
- [CVE-2016-7639](#)
- [CVE-2016-7640](#)
- [CVE-2016-7641](#)
- [CVE-2016-7642](#)
- [CVE-2016-7645](#)
- [CVE-2016-7646](#)
- [CVE-2016-7648](#)
- [CVE-2016-7649](#)
- [CVE-2016-7654](#)
- [CVE-2016-7589](#)
- [CVE-2016-7656](#)
- [CVE-2016-7592](#)
- [CVE-2016-7598](#)
- [CVE-2016-7599](#)

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India