CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Apple iOS

Original Issue Date: 16th May 2017

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Apple iOS and they can be exploited by remote attackers to cause execution of arbitrary code, gain knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Multiple vulnerabilities in Apple Safari **CVE Info:** CVE-2017-2495 CVE-2017-2496 CVE-2017-2499 CVE-2017-2500 List of other CVE Information is available on: https://support.apple.com/en-us/HT207804	Multiple vulnerabilities have been identified in Apple Safari and can be exploited by remote attackers to cause the execution of arbitrary code to be executed on the target user's system. The vulnerabilities can allow remote attackers to cause denial of service conditions, bypass code signing security restrictions, spoof URLs and conduct cross-site scripting attacks. The vulnerabilities reported are as follows: • A remote user can trigger a memory handling error in Safari's history menu to cause denial of service conditions. • A remote user can create a specially crafted website that, when loaded by the target user, will trigger a state management flaw and spoof the address bar.	Apple Safari versions prior to 10.1.1	Users are advised to apply updates. More information about the updates is available on: https://support.apple.com/en-us/HT207804

	• A remote user can trigger a memory corruption error in the WebKit component to execute arbitrary code. • A remote user can trigger a logic error in the WebKit component to conduct cross site scripting attacks. • A remote user can trigger a memory corruption error in the WebKit component to execute arbitrary code. • An application can trigger a memory corruption error in the WebKit Web Inspector component to execute unsigned code.		
Multiple Vulnerabilities in Apple iOS **CVE Info:** CVE-2017-6989 CVE-2017-6982 CVE-2017-2498	Several vulnerabilities have been identified in Apple iOS and can be exploited by remote attackers to cause a denial of service condition, obtain elevated privileges and bypass certificate validation on the vulnerable systems. The vulnerabilities reported are as follows: • The vulnerability exists because an n application can trigger a memory corruption error in the AVEVideoEncoder component to gain kernel-level privileges. • Another vulnerability exists because the application can trigger a memory handling error in Notifications to cause	Apple iOS prior to 10.3.2	Users are advised to apply updates. More information about the updates is available on: https://support.apple.com/en-us/HT207798

	denial of service conditions on the target system. • An unspecified certificate validation error may occur in the Security component.		
Multiple Vulnerabilities in Mac OS / Mac OS X **CVE Info:** CVE-2017-6991 CVE-2017-6990 CVE-2017-6988 CVE-2017-6987 List of other CVE Information is available on: https://support.apple.com/en-us/HT207797	Multiple vulnerabilities were reported in Apple MacOS/OS X and they can be exploited by remote attackers to cause execution of arbitrary code, obtain potentially sensitive information from system memory, obtain elevated privileges on the target system and obtain 802.1X authentication credentials. The vulnerabilities reported are as follows: • An application can exploit a validation flaw in the CoreAudio component to read restricted memory. • An application can trigger an input validation flaw in the HFS component to read restricted memory. • An application can trigger an input validation flaw in the kernel to read restricted memory. • An application can trigger an input validation flaw in the WindowServer component to read restricted memory. • A remote user on a local network can exploit a certificate validation flaw in	Apple MacOS/ OS X versions prior to 10.12.5	Users are advised to apply updates. More information about the updates is available on: https://support.apple.com/en-us/HT207797

	EAP-TLS when a certificate is changed to obtain 802.1X authentication credentials. • An application can trigger a memory corruption error in the Accessibility Framework component to gain system privileges. • A memory corruption error in the CoreAnimation component may allow arbitrary code execution. • A memory corruption error in the TextInput component may allow arbitrary code execution. • An application can trigger a race condition in the DiskArbitration component to gain system privileges. • A remote user can create a specially crafted iBook that, when loaded by the target user, will open arbitrary websites. • An application can exploit a symbolic link (symlink) path validation flaw in iBooks to execute arbitrary code with root privileges. • An application can trigger a memory corruption error in the iBooks component to gain kernel-level privileges.		

	• An application can trigger a memory corruption error in the Intel Graphics Driver component to gain kernel-level privileges . • An application can trigger a memory corruption error in the IOGraphics component to gain kernel-level privileges. • An application can trigger a memory corruption error in the IOSurface component to gain kernel-level privileges. • An application can trigger a memory corruption error in the kernel to gain kernel-level privileges. • An application can trigger a race condition in the kernel to execute arbitrary code with kernel-level privileges. • An application can trigger a memory corruption error in the Multi-Touch component to gain kernel-level privileges. • An application can trigger a memory corruption error in the NVIDIA Graphics Drivers component to gain kernel-level privileges. • An application can trigger a memory corruption error in the Sandbox component to escape its sandbox.		

	• An application can trigger a memory corruption error in the Security component to escape its sandbox. • An application can trigger a memory corruption error in the Speech Framework component to escape its sandbox. • A user-after-free memory error and code execution may occur in the SQLite component in processing specially crafted SQL queries. • A buffer overflow and code execution may occur in the SQLite component in processing specially crafted SQL queries. • A memory error and code execution may occur in the SQLite component in processing specially crafted SQL queries. • A remote user can create specially crafted web content that, when loaded by the target user, will trigger memory corruption errors in SQLite and execute arbitrary code on the target user's system. • An application can trigger a memory corruption error in the Window Server component to gain system		

	privileges.		

Source:

Apple Security Update

https://support.apple.com/en-us/HT207797

https://support.apple.com/en-us/HT207798

https://support.apple.com/en-us/HT207804

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu