Security Advisory | Volume 2019-07-02

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Apple iOS <12.4 Unspecified Vulnerability in Heimdal - CVE-2018-16860	Apple iOS before 12.4 is prone to a vulnerability in Heimdal due to an issue in Samba which could allow attackers to perform unauthorized actions by intercepting communications between services.	iOS <12.4	Vendor - Apple CVE Id - CVE-2018-16860 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210346
HAProxy <=2.0.2 Remote DoS Vulnerability - CVE-2019-14241	HAProxy through 2.0.2 allows attackers to cause a denial of service (ha_panic) via vectors related to htx_manage_client_side_cookies in proto_htx.c.	HA Proxy <=2.0.2	Vendor - HAProxy CVE Id - CVE-2019-14241 CVSS Base - 7.5 Reporting Date - 07/23/2019 Vendor's Advisory - https://github.com/haproxy/haproxy/issues/181
Apple Unspecified Vulnerability in Heimdal - CVE-2018-16860	Apple is prone to a vulnerability in Heimdal due to an issue in Samba which could allow attackers to perform unauthorized actions by intercepting communications between services.	Apple iOS <12.4 Apple Watch OS <5.3 Apple MacOS X <10.14.6	Vendor - Apple CVE Id - CVE-2019-16860 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210346
Apple Remote Code Execution or DoS Vulnerability in Foundation - CVE-2019-8641	Apple is prone to a remote code execution or denial of service vulnerability in the Foundation framework due to an out-of-bound memory read. A remote attacker could exploit this issue to execute arbitrary code or crash the operative application on the affected system.	Apple MacOS X <10.14.6 Apple tvOS <12.4	Vendor - Apple CVE Id - CVE-2019-8641 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210348
Apple MacOS X <10.14.6 Remote Code Execution Vulnerability in FaceTime - CVE-2019-8648	Apple MacOS X before 10.14.6 is prone to a remote code execution vulnerability in FaceTime due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system.	MacOS X <10.14.6	Vendor - Apple CVE Id - CVE-2019-8648 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210348
Apple tvOS <12.4 Remote Code Execution Vulnerability in Core Data - CVE-2019-8647	Apple tvOS before 12.4 is prone to a remote code execution vulnerability in the Core Data component. A remote attacker could exploit this issue to execute arbitrary code on the affected system.	Apple tvOS <12.4	Vendor - Apple CVE Id - CVE-2019-8647 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210351
Apple Remote Code Execution or DoS Vulnerability in Core Data - CVE-2019-8660	Apple is prone to a remote code execution or denial of service vulnerability in the Core Data component due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code or crash the operative application on the affected system.	MacOS X <10.14.6 Apple tvOS<12.4	Vendor - Apple CVE Id - CVE-2019-8660 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210348
Apple MacOS X <10.14.6 Remote Code Execution Vulnerability in Carbon Core - CVE-2019-8661	Apple MacOS X before 10.14.6 is prone to a remote code execution vulnerability in the Carbon Core component due to a use-after-free. A remote attacker could exploit this issue to execute arbitrary code on the affected system.	MacOS X <10.14.6	Vendor - Apple CVE Id - CVE-2019-8661 CVSS Base - 9.8 Reporting Date - 07/22/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210348
Apple Remote Code Execution Vulnerability in WebKit - CVE-2019-8689,CVE-2019-8688,CVE-2019-8687,CVE-2019-8686,CVE-2019-8685,CVE-2019-8684, CVE-2019-8683,CVE-2019-8681,CVE-2019-8680,CVE-2019-8679,CVE-2019-8678, CVE-2019-8677,CVE-2019-8675,CVE-2019-8672,CVE-2019-8671,CVE-2019-8669,CVE-2019-8666,CVE-2019-8644	Apple is prone to a remote code execution vulnerability in WebKit due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system by enticing the user to visit a maliciously crafted webpage.	Apple iCloud <7.13 and <10.6 Apple iTunes <12.9.6	Vendor - Apple CVE Id - CVE-2019-8689,CVE-2019-8688,CVE-2019-8687,CVE-2019-8686,CVE-2019-8685,CVE-2019-8684, CVE-2019-8683,CVE-2019-8681,CVE-2019-8680,CVE-2019-8679,CVE-2019-8678, CVE-2019-8677,CVE-2019-8675,CVE-2019-8672,CVE-2019-8671,CVE-2019-8669,CVE-2019-8666,CVE-2019-8644 VSS Base - 8.8 Reporting Date - 07/23/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210357
Apple Remote Code Execution Vulnerability in WebKit - CVE-2019-8688	Apple is prone to a remote code execution vulnerability in WebKit due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system by enticing the user to visit a maliciously crafted webpage.	Apple iCloud <7.13 and <10.6 Apple iTunes <12.9.6	Vendor - Apple CVE Id - CVE-2019-8688 CVSS Base - 8.8 Reporting Date - 07/23/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210357
Apple Remote Code Execution Vulnerability in WebKit - CVE-2019-8687	Apple is prone to a remote code execution vulnerability in WebKit due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system by enticing the user to visit a maliciously crafted webpage.	Apple iCloud <7.13 and <10.6 Apple iTunes <12.9.6	Vendor - Apple CVE Id - CVE-2019-8687 CVSS Base - 8.8 Reporting Date - 07/23/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210356
Apple iTunes for Windows <12.9.6 Remote Information Disclosure Vulnerability in libxslt - CVE-2019-13118	Apple iTunes for Windows before 12.9.6 is prone to a remote information disclosure vulnerability in libxslt. A remote attacker could exploit this issue to obtain sensitive information on the affected system.	iTunes for Windows <12.9.6	Vendor - Apple CVE Id - CVE-2019-13118 CVSS Base - 7.5 Reporting Date - 07/23/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210356
GoURL <=1.4.13 for WordPress Remote File Upload Vulnerability in gourl.php - CVE-2019-1010209	GoUrl.io GoURL Wordpress Plugin 1.4.13 and earlier is vulnerable to unauthenticated and unauthorized attackers uploading executable files to a website. The affected code is at gourl.php#L5637. The fixed version is: 1.4.14.	GoURL Plugin <=1.4.13	Vendor - Apple CVE Id - CVE-2019-13118 CVSS Base - 7.5 Reporting Date - 07/23/2019 Vendor's Advisory - https://github.com/cryptoapi/Bitcoin-Wordpress-Plugin/blob/8aa17068d7ba31a05f66e0ab2bbb55efb0f60017/gourl.phpL5637