Security Advisory Report - OBSO-1903-01

Google WebRTC RTCPeerConnection Object Handling Use-after-free Arbitrary Code Execution (CVE-2019-6211)

Release Date:	2019-03-04 17:39:11
Last Update:	2019-03-04 17:56:29

Summary

Google WebRTC contains a use-after-free error that is triggered when handling a specially crafted RTCPeerConnection object. This may allow a context-dependent attacker to dereference already freed memory and potentially execute arbitrary code.

Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Apple Safari. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the handling of RTCPeerConnection objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process.

https://www.zerodayinitiative.com/advisories/ZDI-19-127/

Fixed in Apple IOS 12.1.3

Fixed in macOS 10.14.3

Affected Products

Affected products

Circuit Mobile Client (IOS)

According to https://support.apple.com/en-us/HT209443 this issue affected iOS devices but was addressed in the iOS update 12.1.3 released January 22, 2019.

Not affected products:

Circuit Mobile Client (Android)

Branch/ SBC

myPortal@work

All other products do not use WebRTC

Recommended Actions

Apply iOS update 12.1.3 for Circuit Mobile Client (IOS)

References

https://support.apple.com/en-us/HT209443

https://support.apple.com/en-us/HT209446

https://www.zerodayinitiative.com/advisories/ZDI-19-127/

https://seclists.org/fulldisclosure/2019/Jan/62

Advisory: OBSO-1903-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.