



# Security Advisory Report - OBSO-1705-01

## Race condition in Chrome (CVE-2017-5068)

Creation Date: 2017-05-23  
Last Update: 2017-05-23

### Summary

WebRTC library/project contains an unspecified race condition that is triggered during the handling of frame orders. This may allow a context-dependent attacker to have an unspecified impact. No further details have been provided.

The vulnerability is potentially exploitable, but there is currently no known way to do so.

### Vulnerability Details

#### WebRTC:

The bug was introduced in WebRTC rev-16772. Currently, there are no known workarounds or upgrades to correct this issue. However, a patch has been committed to the source code repository (e.g. GIT, CVS, SVN) that addresses this vulnerability. Until it is incorporated into the next release of the software, manually patching an existing installation is the only known available solution.

WebRTC is part of Google Chrome  
**Google Chrome** fix version: 58.0.3029.96

IE, Edge and Firefox are not affected.

There is a fix for **openSUSE**:  
<https://www.suse.com/security/cve/CVE-2017-5068/>

### Affected Products

**Circuit web client:** Please update to latest stable channel of Chrome (58.0.3029.96 or newer).

**Circuit Desktop** app: not affected.

**Circuit Meeting Room:** CMR updates Chrome automatically. We suggest customers to check and update the Chrome (to 58.0.3029.96 or newer) using dashboard of CMR

**Circuit Mobile Client (Android) V1:** not affected.  
**Circuit Mobile Client (iOS) V1:** not affected.

**OpenScape Branch/SBC V8 R1:** not affected  
**OpenScape Branch/SBC V9:** not affected

**OpenScape Mobile** OSMO client (Android): not affected

### Recommended Actions

This vulnerability was introduced with Chrome 58. Older versions are not affected

Fix for Chrome: The stable channel has been updated to **58.0.3029.96** for Windows, Mac, and Linux.

<https://chromereleases.googleblog.com/2017/05/stable-channel-update-for-desktop.html>

**Customers are advised to update Google Chrome.**

## References

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5068>

<https://chromereleases.googleblog.com/2017/05/stable-channel-update-for-desktop.html>

<https://groups.google.com/forum/#!msg/discuss-webrtc/pfwS9eeS23c/x6qCSzW8BAAJ>

## Revision History

First draft: 2017-05-12

First Release 2017-05-23

---

Advisory ID: OBSO-1705-01 (a=163), 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

[obs@unify.com](mailto:obs@unify.com)

© Unify Software and Solutions GmbH & Co. KG 2017

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

[www.unify.com](http://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.