# Security Advisory Report - OBSO-1611-01

## Dirty Cow: Linux Kernel MAP_PRIVATE COW Flag Breakage Race Condition (CVE-2016-5195)

Creation Date: 2016-11-03 12:45:58
Last Update: 2018-06-01 15:54:15

## Summary

Update #6:

OpenStage 15/20/40/60, Desk phone IP 33G, 55G SIP V3  use V3 R5.8.2 or later
OpenStage 15/20/40/60, Desk phone IP 35G, 55G HFA V3 use V3 R0.40.3 or later

There is a fix for all products now

A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings.

An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

## Details

Linux Kernel contains a flaw in the follow_page_pte() function in mm/gup.c that is triggered when handling MAP_PRIVATE COW breakage.

The attack relies on racing the madvise(MADV_DONTNEED) system call while having the page of the executable mmapped in memory.

This may allow a local attacker to gain elevated privileges.

The bug has existed since around Linux Kernel  2.6.22 (released in 2007) and was fixed on Oct 18, 2016.

https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

This is a high visibility issue, but it is not necessarily a high priority vulnerability for Unify products.

The vulnerability is only relevant, if a local user access is possible.

If there is no local user access dirty cow can only be exploited if a second vulnerbility is exploited at the same time to get local access.

Cloud services where the user never gets local access are not affected, like above.

If there is only one user in place no privilege escalation is possible.

For products where memory mapping is done in a different way dirty cow is not relevant.

For products where local access is possible Unify provides hardening of the products and security checklists  that includes a password policy.

So an attacker must first hack into the local user account and then exploit dirty cow.

In this case prioriy can be reduced to medium.

## Affected Products

**Affected Products, prioriy is medium to low**

OpenScape Branch and SBC V7, V8, V9
use V9 R1.1.0 or later

OpenScape 4000, 4000 Assistant
V7: use V7 R2.24.0 or later
V8: use V8 R0.14.0 or later

OpenScape Voice V7, V8, V9
OSV V9: use V9 R1.19.2 or later
OSV V8: use V8 R1.49.1 or later
OSV V7: use V7 R1.51.9 or later

Xpert MLC and 6010p/6010p-V1R1 (Linux) Turret.
MLC is an application and delivered without OS, please update OS to include fix.
Turrets: use V5 R1.5.5 or later.

OpenScape Contact Center Call Director SIP Service (CDSS) V9
Use V9 R0.2.0 or later

OpenScape Desk Phones and OpenStage Phones are affected, but with low priority, since an administrator has to log onto the phone and enable
SSH or serial port access, they are disabled by default.

Fix versions:

**OpenStage 15/20/40/60, Desk phone IP 33G, 55G SIP V3  use V3 R5.8.2 or later**
**OpenStage 15/20/40/60, Desk phone IP 35G, 55G HFA V3 use V3 R0.40.3 or later**

OpenScape Desk phone IP 35G Eco SIP V3 use V3 R5.1.0 or later
OpenStage Desk phone IP 35G Eco HFA use V3 R0.39.0 or later

Desk phones CP400/CP600 SIP V1 use V1 R2.5.0 or later
Desk phones CP400/CP600 HFA V1 use V1 R1.9.0 or later

Desk phones CP200 SIP V1 use V1 R2.5.0 or later
Desk phones CP200 HFA V1 use V1 R0.3.0 or later

**Not affected Products:**

OpenScape Office V3 R3

OpenScape Business V2

HiPath Cordless IP Base Station V1 R5, V1 R6

Circuit

OpenScape Alarm Response Economy, Professional

## Recommended Actions

Updates for most affected products are available, they should be applied as soon as available.

## References

Explanation:  http://dirtycow.ninja/

More details:

https://www.linux.com/blog/how-bad-dirty-cow

https://lwn.net/Articles/704231/

Github mit PoCs: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails

Kernel Fix:
https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619

Advisory: OBSO-1611-01, 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