

PUBLIC - FOR EXTERNAL USE: ([TLP: WHITE](#))

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

## Security Advisory Report - OBSO-2203-02

### Linux Kernel lib/iov\_iter.c Multiple Functions Missing Flag Initialization Read-only File Overwrite Local Privilege Escalation (CVE-2022-0847, Dirty Pipe)

Status:	Update Release
Release Date:	2022-03-16 14:20:54
Last Update:	2023-01-16 15:16:23
Version:	1.6

#### Summary

The Linux Kernel contains a flaw in the `copy_page_to_iter_pipe()` and `push_pipe()` functions in `lib/iov_iter.c` that is triggered as the `flag` member of the pipe buffer is not initialized. This may allow a local attacker to overwrite the page cache, allowing to overwrite read-only files and subsequently gain elevated privileges.

The vulnerability affects the Linux kernel starting with version 5.8 and was fixed in the latest kernel versions – namely 5.16.11, 5.15.25, and 5.10.102.

The underlying issue of CVE-2022-0847 (missing initialization) has been present in the kernel since version 4.9. However – the only currently known vector for exploitation (the use of the `PIPE_BUF_FLAG_CAN_MERGE`) was introduced in version 5.8. As such Linux kernel versions between 4.9 and 5.7 could be exploited in the future through a different vector, but none of the current exploits work on these versions.

The vulnerability is rated high for products that use kernel version 5.8 and lower than the fixed version 5.16.11, 5.15.25, and 5.10.102.

At present no Atos Unify products are affected with high severity.

The vulnerability is rated medium for products that use kernel versions 4.9 to 5.7.

#### Details

The CVSS base core is high: 7.8 (applies to affected Kernel version 5.8 and higher)

[CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H](#)

For Kernel versions 4.9 - 5.7 we rate the vulnerability with a Temporal score of medium: 6.6

[CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:U](#)

## Affected Products

Atos Unify products that are considered appliances with an embedded linux operating systems are under investigation.

Atos **Unify applications that are installed on a Linux operating systems** that is not embedded within the product are considered as **confirmed not affected**. Customer should follow the instructions of the Linux operating system provider and apply the patches that are provided. Atos Unify will not deliver updates for Linux based applications.

Atos Unify applications that are installed on Windows operating systems are not affected.

### Products confirmed affected (medium)

#### *Linux based appliances*

Atos Unify OpenScape Voice (simplex deployments) V9 an V10  
Atos Unify OpenScape Voice (duplex deployments) V9 an V10 (fixed in V10R2.14.0 / available)  
Atos Unify OpenScape Cordless IP V2 fix planned on H2 of 2023  
Atos Unify OpenScape First Response ESRP V9 before V9 R4.66.0  
Atos Unify OpenScape First Response BCF V10 befor V10R10.0.0  
Atos Unify OpenScape Xpert Clients V6 and V7 (fixed in V7.4.1.0 / no fix planned for V7 R3)  
Atos Unify OpenScape Branch V9 and V10 (fixed in V10R2.3.0 /available  
Atos Unify OpenScape SBC V9 and V10 (fixed in V10R2.4.0 /available)  
Atos Unify OpenScape Contact Media Service V10,V11 (fixed in V11R0.2.0 / available)

#### *Solutions and Cloud Services*

##### Circuit

Atos Unify OpenScape Business V3  
Atos Unify OpenScape Enterprise Express V9 and V10

### Products confirmed not affected

#### *Linux based appliances*

Atos Unify OpenScape 4000 V8 and V10 Platform  
Atos Unify OpenScape 4000 V8 and V10 Assistant  
Atos Unify OpenScape 4000 V8 and V10 CSTA  
Atos Unify OpenScape 4000 V8 and V10 Loadware  
Atos Unify OpenScape First Response ESAPP V1  
Atos Unify OpenScape First GEMMA V3  
Atos Unify OpenScape Alarm Response Professional V4 and V5  
Atos Unify Virtual Care Collaboration Service V1  
Atos Unify OpenScape Desk Phones CP SIP  
Atos Unify OpenScape Desk Phones CP HFA  
Atos Unify OpenScape Desk Phones IP SIP V3  
Atos Unify OpenScape Desk Phones IP HFA V3  
OpenStage HFA V3

OpenStage SIP V3

Atos Unify OpenScape WLAN Phone WL3 and WL4

Atos Unify OpenScape DECT Phone S5 and S6

Atos Unify OpenScape DECT Phone SL5 and SL6

Atos Unify OpenScape WLAN Phone Wireless Service Gateway

*Linux based applications (follow instructions of the Linux operating system providers)*

Atos Unify OpenScape First Response MSBF V2

Atos Unify OpenScape Xpert MLC V6 and V7

Atos Unify OpenScape UC Application V9 and V10

Atos Unify OpenScape Media Server V9

Atos Unify OpenScape 4000 Manager V8 and V10

Atos Unify OpenScape Common Management Platform V7 and V10

Atos Unify OpenScape Composer V2

Atos Unify OpenScape Voice Survival Authority

Atos Unify OpenScape Backup & Recovery Services

HiPath CAP V3.0

*Applications that may be deployed on Windows or Linux (for Linux deployments check patches of Linux providers)*

Atos Unify OpenScape License Management CLA/CLM

*Windows based applications*

Atos Unify OpenScape Xpert System Manager V6 and V7

Atos Unify OpenScape Contact Center V10,V11

Atos Unify OpenScape Contact Center Extensions V3

Atos Unify OpenScape Fusion for Office V1 and V2

Atos Unify OpenScape Extensions for MS Outlook V1 and V2

Atos Unify OpenScape Fusion for Notes V1 and V2

Atos Unify OpenScape Web Collaboration V7

Atos Unify OpenScape Concierge V4

Atos Unify OpenScape Xpressions V7

Atos Unify OpenScape Personal Edition V7

Atos Unify OpenScape Deployment Service V7 and V10

Atos Unify OpenScape Fault Management V10, V11 and V12

Atos Unify OpenScape Accounting Management V3, V4 and V5

Atos Unify OpenScape Voice Trace Manager V8

AC Win SL V3

HiPath DS-Win V4

Atos Unify OpenScape Sesap V2

## Recommended Actions

### For Linux based appliances, Solutions and Cloud Services that are affected

- Patches will be provided with the next regular patch cycle

### For Atos Unify applications using affected Linux operating systems:

- Check operating systems providers recommendation
- Apply the patches that are provided

## References

### External References

- [CVE-2022-0847: DirtyPipe Vulnerability Technical Overview \(jfrog.com\)](#)
- <https://dirtypipe.cm4all.com/>
- <http://packetstormsecurity.com/files/166258/Dirty-Pipe-Local-Privilege-Escalation.html>
- <https://dirtypipe.cm4all.com/>
- <https://jfrog.com/blog/dirtypipe-cve-2022-0847-the-new-dirtycow/>
- [CVE-2022-0847 | SUSE](#)
- [List of SUSE Linux Enterprise Server kernel \(version and release date\) | Support | SUSE](#)
- [openSUSE - Wikipedia](#)
- <https://security-tracker.debian.org/tracker/CVE-2022-0847>
- <https://www.suse.com/support/update/announcement/2022/suse-su-20220755-1/>
- <https://www.suse.com/support/update/announcement/2022/suse-su-20220757-1/>
- <https://www.suse.com/support/update/announcement/2022/suse-su-20220759-1/>
- <https://www.suse.com/support/update/announcement/2022/suse-su-20220760-1/>
- [Debian version history - Wikipedia](#)
- <https://www.debian.org/security/2022/dsa-5092>
- <https://ubuntu.com/security/CVE-2022-0847>
- <https://ubuntu.com/security/notices/USN-5317-1>

## Version Change History

Version	Date	Description
1.0	16.03.2022	- Initial release
1.1	22.03.2022	- OpenScape First GEMMA V3 is not affected

Version	Date	Description
1.2	18.05.2022	<ul style="list-style-type: none"> <li>- OpenScape Branch and OpenScape SBC fixed planned in V10R2.3.0 for 27.5.2022</li> <li>- OpenScape Voice fix planned in V10R2.14.0 for 08/2022</li> <li>- OpenScape Contact Media Service fix planned in V11R0.2.0</li> <li>- OpenScape Cordless IP fix planned in V2 R2 for 06/2022</li> <li>- Xpert Clients fixed in V7.4.1.0 / fix planned in V7.3.4.0 for 20.5.2022</li> </ul>
1.3	07.06.2022	<ul style="list-style-type: none"> <li>- OpenScape SBC fixed in V10R2.4.0 / available</li> <li>- OpenScape Branch fixed in V10R2.3.0 / available</li> <li>- OpenScape Contact Media Service fixed in V11R0.2.0 / available</li> <li>- OpenScape Xpert V7 R3 : statement in clarification)</li> <li>- Correction for OpenScape Cordless IP V2 (no plan date yet)</li> </ul>
1.4	12.08.2022	- OpenScape Voice fixed in V10R2.14.0
1.5	08.11.2022	- OpenScape BCF fixed in V10R10.0.0
1.6	16.01.2023	<ul style="list-style-type: none"> <li>- No fix planned for OpenScape Xpert Clients V7 R3</li> <li>- OpenScape First Response ESRP V9 fixed in V9 R4.66.0</li> <li>- Atos Unify OpenScape Cordless IP V2 fix planned on H2 of 2023</li> </ul>

Advisory: OBSO-2203-02, status: update release

Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see <https://www.unify.com/security/advisories>.

Contact and Disclaimer

### **OpenScape Baseline Security Office**

[obso@atos.net](mailto:obso@atos.net)

© Unify Software and Solutions GmbH & Co. KG 2023

Otto-Hahn-Ring 6

D-81739 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.