

# Security Advisory Report - OBSO-2209-01

## Realtek eEcos SDK vulnerability (CVE-2022-27255)

Release Date: 2022-09-05 15:53:46  
Last Update: 2022-09-05 16:25:53  
Version: 1.0

### Summary

A critical vulnerability recorded as CVE-2022-27255 has been identified that affects products using the Realtek eCos SDK used within the RealTek RTL819x family of System on Chip devices. A remote attacker can cause a buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code. We are evaluating our portfolio whether the RealTek RTL819x family of System on Chip devices is used.

At present no supported product has been identified as using the affected chipset. Check the Affected Products sections for details of the evaluated products.

### Details

Additional information is available in the References section of the Security Advisory.

### Affected Products

Product statements are related to product versions before End of Support (M44) is reached

#### Products confirmed not affected

*Products delivering hardware that have been evaluated*

Atos Unify OpenScape Business V3  
Atos Unify OpenScape 4000 V8 and V10 Platform  
Atos Unify OpenScape 4000 Ecoserver  
Atos Unify OpenScape Ecoserver  
Atos Unify OpenScape 4000 Branch  
Atos Unify OpenScape EcoBranch  
Atos Unify OpenScape 4000 DSCXLV2  
Atos Unify OpenScape 4000 STMIX  
Atos Unify OpenScape Access 500  
Atos Unify OpenScape Cordless IP V2  
Atos Unify OpenScape First Response BCF V10  
Atos Unify OpenScape Xpert Clients V7  
Atos Unify OpenScape Branch V10  
Atos Unify OpenScape SBC V10

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  
Atos Unify OpenScape WLAN Phone WL3 and WL4  
Atos Unify OpenScape DECT Phone S5 and SL5  
Atos Unify OpenScape DECT Phone R6, S6 and SL6  
Atos Unify OpenScape WLAN Phone Wireless Service Gateway

*Software only products and solutions are not affected*

Atos Unify OpenScape Enterprise Express V10  
Atos Unify OpenScape Voice (simplex deployments) V10  
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 Voice (duplex deployments) V10  
Atos Unify OpenScape First Response ESRP V9  
Atos Unify OpenScape First Response ESAPP V1  
Atos Unify OpenScape First Response PSS V1  
Atos Unify OpenScape First Response MSBF V2  
Atos Unify OpenScape First GEMMA V3  
Atos Unify Virtual Care Collaboration Service V1  
Atos Unify OpenScape Xpert MLC V7  
Atos Unify OpenScape Xpert System Manager V7  
Atos Unify OpenScape Contact Center V10,V11  
Atos Unify OpenScape Contact Media Service V10,V11  
Atos Unify OpenScape UC Application V10  
Atos Unify OpenScape Fusion for Office V2  
Atos Unify OpenScape Extensions for MS Outlook V2  
Atos Unify OpenScape Fusion for Notes 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 Media Server V9  
Atos Unify OpenScape 4000 Manager V8 and V10  
Atos Unify OpenScape Common Management Platform V10  
Atos Unify OpenScape Composer V2  
Atos Unify OpenScape Deployment Service V10  
Atos Unify OpenScape Fault Management V11 and V12  
Atos Unify OpenScape Accounting Management V4 and V5  
Atos Unify OpenScape Voice Trace Manager V8  
Atos Unify OpenScape Voice Survival Authority  
AC Win SL V3  
HiPath CAP V3.0  
HiPath DS-Win V4  
Atos Unify OpenScape Backup & Recovery Services  
Atos Unify OpenScape Sesap V2

Atos Unify OpenScope License Management CLA/CLM

Services

Circuit

### Products under investigation

Atos Unify OpenScope Alarm Response Professional V4 and V5

## Recommended Actions

At present no further action is required for Atos Unify products.

## References

- <https://nvd.nist.gov/vuln/detail/CVE-2022-27255>
- <https://www.bleepingcomputer.com/news/security/exploit-out-for-critical-realtek-flaw-affecting-many-networking-devices/>
- <https://www.scmagazine.com/brief/device-security/vulnerability-in-realtek-ecos-sdk-poses-threat-to-networking-devices>
- <https://www.securityweek.com/realtek-sdk-vulnerability-exposes-routers-many-vendors-remote-attacks>
- 

## Version Change History

Version	Date	Description
1.0	05.09.2022	- Initial release

---

Advisory: OBSO-2209-01, status: general 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

**OpenScope Baseline Security Office**

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

© Unify Software and Solutions GmbH & Co. KG 2022

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.