# Security Advisory Report - OBSO-2101-02

## OpenScape Business S - WAN Interface Vulnerability

| | |
|---|---|
| Release Date: | 2021-01-19 16:07:36 |
| Last Update: | 2021-01-19 19:20:34 |

## Summary

If the WAN interface of OpenScape Business S is directly connected to an internet service provider (ITSP), WAN interface ports will be directly exposed to the Internet. An attacker could use this behaviour and try to get access to the system from the Internet and exploit the system.

The WAN interface of OpenScape Business S must be connected via TCP/IP to an external router with NAT and appropriate firewall settings, if the connected ITSP supports beneath telephony data also Internet access.

The vulnerability is rated high and immediate action is recommended.

## Details

Within OpenScape Business S systems a second LAN interface card can be added and configured as WAN interface. The WAN interface is intended for the connection of Internet Telephony Service Provider (ITSP) only. Internet access has to be done always via an Internet Router connected to the LAN interface of OpenScape Business S.

OpenScape Business S WAN interface can be connected either directly to an DSL or cable modem or alternatively via TCP/IP to an external router. In case that the WAN interface is configured as “Connection to a DSL or cable modem” Network Address Translation (NAT) is not supported for the WAN interface and the same firewall rules as defined for the LAN interface are applied.

Some Internet providers (e.g. Vodafone) offer ITSP trunks with a public IP address that provides also Internet data traffic beside the pure telephony traffic.In case that such kind of ITSP trunk is connected directly (without external Internet router) to the WAN interface of OpenScape Business the system is visible within the Internet. As a public address is used and data traffic is not limited to voice data only by the provider the system can be accessed from any place in the world without any restrictions.

An attacker can scan the system from the Internet and try to intrude into the system and to compromise the system and potentially also other systems in the customer LAN.

## Affected Products

### Affected products

OpenScape Business S versions V1, V2 and V3

**Not affected products**

OpenScape Business X systems are not affected.

## Recommended Actions

Connect OpenScape Business S Systems WAN interface via TCP/IP connection and an external router to the ITSP.

For OpenScape Business S on-premise:
Use NAT within the router and open only the ports used for Internet Telephony in the firewall of the router.

For OpenScape Business S in the Cloud:
The firewall from the cloud provider can be used, permitting access to certain ports only.

## References

**OpenScape Business Administrator Manual:**
Downloadable as PDF file via the Service Center of the OpenScape Business Administration Portal (WBM).

**How To Configure LAN-WAN Interfaces for VoIP**
Downloadable as PDF file within the following link:
https://wiki.unify.com/wiki/OpenScape_Business#Configuration_of_LAN.2FWAN_interface_for_VoIP

---

Advisory: OBSO-2101-02, 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

***OpenScape Baseline Security Office***
***obso@atos.net***

***Otto-Hahn-Ring 6***
***D-81739 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.