Security Advisory Report - OBSO-2110-01

Atos Unify Product Security Configuration Note

Release Date:	2021-10-14 14:21:54
Last Update:	2021-10-14 14:21:54

Summary

The following security configuration note for Atos Unify Products and the Atos Unify Session Border Controller emphasizes important configuration steps that are essential to for a secure configuration of the products. It is the result of evaluations that the product configuration has not been done according to Atos Unify recommendations.
Refer to the current Security Checklist of the respective product for a comprehensive coverage of recommended security measures.

Details

1. General Recommendations:

Requirements that are relevant for all Atos Unify products:

- Make sure that implementation is done according to the instructions given in the latest installation guide and configuration guide that is available for the product
- Implement measures according to the latest **Security Checklist** that is part of the product documentation
- Always change the default administrative passwords and frequently change passwords according the applicable password policies of the customer/service provider
- Do not directly expose administrative interfaces to the internet without additional security measures in place
- If remote administration is required use a secure administration platform like the Atos Unify Remote Service Platform

2. Specific Recommendation for OpenScape Session Border Controller:

a) Best practice configuration (recommended)

- It is recommended to integrate a centralized SBC into the customer's DMZ. (Demilitarized Zone)
- Separate WAN and LAN interface of the Session Border Controller and integrate them into different IP networks
- Do not expose the administration interface to the WAN interface
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller

b) Alternate "Single Arm Configuration" without external access to administrative interfaces (not recommended)

In case LAN and WAN interface of the Session Border Controller are connected to the same interface

- Always use an external firewall to restrict access to the Session Border Controller
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall
- Restrict access on administrative interfaces for https, snmp, ssh in the firewall configuration of the Session Border Controller

c) Alternate configuration with external access to administrative interfaces (not recommended)

- Use an overlay vpn solution to provide administrative access (e.g. Atos Unify Remote Service Platform or similar solution)

or

- Always use an external firewall to restrict access to the Session Border Controller
- Disable access to administrative interfaces (https, ssh, snmp) of the Session Border Controller from the external firewall
- Enable administrative access on the external firewall on demand for the time that access is needed and for ip addresses that require access
- Implement additional security measures as two-factor authentication, encrypted connections etc.

Affected Products

- The General Recommendations apply to all Atos Unify products.
- The Specific Recommendations apply to OpenScape Session Border Controller Version 9 and 10.

Recommended Actions

- Check current configuration in particular change the default passwords as recommended.
- Check current configuration and implement necessary improvements.

References

Advisory: OBSO-2110-01, 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

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.