Security Advisory Report - OBSO-2107-02

Update of Security Checklist for Atos Unify OpenScape Alarm Response

Release Date:	2021-07-26 16:30:02
Last Update:	2021-07-26 16:55:21

Summary

This information advisory is released in order to inform about an important update of the Security Checklist for Atos Unify OpenScape Alarm Response as part of the release of version 5. In order to protect OpenScape Alarm Response solutions against Denial of Service attacks it is recommended to use a Next Generation Firewall including Intrusion Prevention capabilities. A tradition firewall solely relying on packet filtering capabilities is not considered sufficient to protect the solution.
Please refer to Details for additional information and section 8.3 of the Security Checklist for OpenScape Alarm Response V5.

Details

Excerpt from Security Checklist OpenScape Alarm Response version 5 :

OScAR / DAKS is designed to be used in security protected data center environments with proper state of the art IT-Security measures in place. As network and IT-Security related threats are growing worldwide we wanted to highlight a specific OScAR / DAKS feature, too.

In addition to numerous safety and security features, OScAR / DAKS incorporates a special watchdog capability to ensure deterministic behavior of the system even in case of unlikely and unforeseeable events. Therefore, the watchdog process internally observes several criteria, whereof specifically external network traffic load (e.g. a DoS attack) is an important criterion.

As a security measure the watchdog will in case of an external network overload detection finally initiate a reboot, to mitigate threats and to behave deterministic. In addition, the feature triggers the deactivation of the build-in last error message relay contact for an alerting.

The outcome of scenarios like that may cause services being temporarily unavailable on the network layer, which would be the case anyway if such attacks happen inside an internal network.

This type of last line of defense against unwanted behavior is a works-as-designed feature and is important for the overall deterministic reliability and purpose of usage.

Affected Products

Atos Unify OpenScape Alarm Response Version 4 and 5

Recommended Actions

Since 2010 the firewall concepts that are mainly limited to port filtering have evolved to include more and more inspection capabilities for higher OSI layer protocols too. Back than the expression next generation firewall (3rd generation firewall) was established.

As of 2021 next generation firewall concepts are state-of-the-art and predominantly used in corporations. Combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS) (see https://en.wikipedia.org/wiki/Next-generation_firewall), and Intrusion Detection (IDS) offers more features.

In order to best prevent cyber attacks that use Denial of Service (DoS) or random trash data attacks (DoS with fuzzing) – for details see https://en.wikipedia.org/wiki/Fuzzing; https://en.wikipedia.org/wiki/Denial-of-service_attack) – next generation firewall concepts shall be used. The expression firewall and next-generation firewall (NGFW) are usually used synonymously.

Interfaces, which are not used, are deactivated by default, and shall not be activated without explicit need. The ports used by OScAR V5 can be found in the addendum. This information may be used for external firewall configuration e.g. for network separation to increase security.

A firewall /next generation firewall utilizing in-line deep packet inspection (DPI), intrusion detection system (IDS) and intrusion prevention system (IPS) capabilities shall be configured properly to prevent threats from cyber-attacks.

References

Reference to the Security Checklist: published after the release

https://en.wikipedia.org/wiki/Next-generation_firewall

https://en.wikipedia.org/wiki/Fuzzing; https://en.wikipedia.org/wiki/Denial-of-service_attack)

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com