Security Advisory Report - OBSO-2009-01

SSH configuration vulnerability within OpenScape 4000

Release Date:	2020-09-08 11:43:09
Last Update:	2020-09-08 11:55:55

Summary

The default SSH configuration of OpenScape 4000 supports outdated key exchange algorithms using sha-1, that may allow an attacker to compromise key exchange while a SSH session is established. The vulnerability affects OpenScape 4000 versions V10, V8 and earlier versions, refer to the details listed below.

The vulnerability is rated medium.

Details

The default SSH configuration supports a number of key exchange algorithms including strong algorithms that are considered secure. If both communication parties support strong algorithms they are preferred when a session is established, The existence of outdated algorithms in the default configuration may allow an attacker to force endpoints to choose weaker algorithms instead and exploit weaknesses of the respective protocols. As SSH interfaces should be restricted to internal protected networks this weakness will be difficult to exploit and effort is considered high. SSH provides strong protection against cipher downgrade attacks, thus offering outdated ciphers on a SSH server bears low risk, if SSH clients all support a secure cipher suite in common with the server.
The affected algorithms are not recommended any longer hence they will be removed in the SSH configuration for OpenScape 4000 V10.

CVSS3.1 Base score: 7.6
CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

CVSS3.1 Temporal score: 6.6
CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Affected Products

Not affected:
OpenScape 4000 V10 platform

Affected
OpenScape 4000 V10 Assistant (Fix available in V10 R0.28.1)
OpenScape 4000 V10 CSTA (Fix planned)

OpenScape 4000 V8 (no fix is planned)
OpenScape 4000 earlier versions (no fixes are planned)

Recommended Actions

Recommendations:

- Upgrade to OpenScape V10 and implement the provided updates for affected components
- Do not publicly expose SSH interfaces to the internet without additional protection in place (e.g. an overlay IPSec connection)
- If you connect from a SSH Client, disable key exchange algorithms that support sha-1

References

Advisory: OBSO-2009-01, 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