Security Advisory Report - OBSO-1410-03

OpenScape Business - Getting Root Access

Creation Date: 2014-10-24
Last Update: 2014-10-26

Summary

A method was published how administrators can achieve 'root' (superuser) privileges on the Linux-based platform of an OpenScape Business V1 system.

The risk for potential misuse of this method is rated low.

Vulnerability Details

A video titled "*OpenScape Business - Getting Root Access*" was uploaded at the Youtube public video portal on 2014-10-21.
Reference: https://www.youtube.com/watch?v=-iXNm71U_TE

It demonstrates a way how an authenticated administrator (expert role) can achieve 'root' (superuser) access on the underlying Linux-based operating system. The steps are

- access an OpenScape Business system V1 R3.1, using the administrator login (expert role)
- enable Secure Shell (ssh) access to the system
- use the lower-privileged Linux user id "postgres" to modify startup files to change the root password in the startup phase
- gain Linux root access after system reboot

Unify rates the risk for potential misuse as low. It requires administrator access, whereby full control of the OpenScape Business system is granted already.
CVSS Scores:

- Base Score: 3.8, Temporal Score: 3.1
- CVSS v2 Vector (AV:A/AC:M/Au:S/C:P/I:P/A:N/E:F/RL:OF/RC:C)

Disclosure timeline:

- 2014-10-21: Video uploaded to public Youtube portal by unknown author
- 2014-10-23: Unify was informed about this video, starts analysis and attempts to contact the author (without success yet)
- 2014-10-24: Unify releases Advisory
- 2014-10-25/26: Author responded; technical clarification and common agreement regarding disclosure and advisory contents

Affected Products

- OpenScape Business V1 (before V1 R3.2)

Recommended Actions

As part of Unify's continuous product security improvements, the relevant issues in the underlying Linux setup (logon to postgres id, weak file access permissions) were already identified internally and solved. The attack described in the video is no longer possible in version V1 R3.2.0.

We recommend customers to

- ensure that only trusted administrators have access to the expert level administration of OpenScape Business and to protect the logon using an individual and strong password
- upgrade to OpenScape Business V1 R3.2.0 (release date: 2014-10-24)

References

Youtube: https://www.youtube.com/watch?v=-iXNm71U_TE

Revision History

2014-10-24: Initial release
2014-10-26: Update 01: No changes, but completion of disclosure timeline

---

Advisory ID: OBSO-1410-03 (a=96), status: update release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com