Security Advisory Report - OBSO-1602-01

OpenScape Accounting Management - Virus Alert in Installation Procedure

Creation Date: 2016-02-05
Last Update: 2016-09-29

Summary

OpenScape Accounting Management (V1 or V2 **before V2 R0.11.0**) may produce a virus alert during installation if an antivirus product is installed on the Windows server.

Risk level: info
This is a security note to confirm that this alert can be seen as a "false positive".

Vulnerability Details

The file "lib\PortOpen.exe" in the installation package of OpenScape Accounting Management (AM) V1 or V2 **before V2 R0.11.0** may be identified as a trojan by various virus scanner products. The name of the trojan can be e.g. "Trojan.GenericKD.3009641", "HEUR/QVM10.1.Malware.Gen", "Win32:Malware-gen", "TR/Rogue.952832.2", "Artemis!B268B7FD3997", or similar malware names.

The file is an intentional part of the installation package. It is a small self-developed application that just checks whether a specific port for a given IP address is available and answers true/false. It is used to determine if the required port 443 for the Web Server is in use during the installation.

We confirm that this file does not contain any malware and has been part of the installation package of OpenScape AM since the first release of V1. The chapter "Recommended Actions" provides some hints how to continue in cases where an alert is raised by a virus scanner product.

Notes:

- We generally recommend to run an antivirus software on Windows-based application servers where products of Unify are installed. The preferred software is the TrendMicro-based "Anti-Virus for OpenScape Servers" as provided by Unify. This solution is also constantly being used for system and release tests of Unify products, thus any potential incompatibilities would be detected at the earliest opportunity. It also does not raise a false-positive alert for "lib\OpenPort.exe".
- **Starting with OpenScape AM V2 R0.11.0 (release date: 2016-02-19) the file has been removed** from the installation package and replaced by an alternate mechanism. This avoids potential false positive alerts in future.

Affected Products

OpenScape Accounting Management V1 and V2, all versions up to and including V2 R0.9.0

Recommended Actions

If your virus scanner raises an alert during installation of OpenScape AM V1 or V2 **before V2 R0.11.0**, you should first verify that the corresponding file ("lib\OpenPort.exe") was not altered in any malicious way after you have retrieved it from Unify's software download server.
The file has a constant size of 952832 bytes and - depending on the compilation time and version - a different checksum, as follows:

OpenScape Accounting Management V1 R2.18.0:

- SHA-256: a7118638a17b5e9a5e41c6efe7e98ad2d3a7c48c9b8a6476e86f1ddd2c409c71
- SHA-1: 8e3a9f4dab22d2fbddcf75d9c2aefbe114ab59f4
- MD5: b268b7fd3997eee01194fe7e3b63e1b1

OpenScape Accounting Management V2 R0.9.0:

- SHA-256: 4bc15aee34d0fa521fd3ae767104aa03ed263370d6f59a2134adcb6ef8d4b635
- SHA-1: b9fd610945a243f558da64f50e57b68afd57f1e2
- MD5: c09f9162cc57c040c37b06d14bd9af91

Verify the file's size and checksum by using either of the available methods (SHA-256, SHA-1 or MD5).
If they match, then there is no risk. Continue installation of OpenScape AM by taking appropriate measures; this depends on the antivirus product in use (for example, define the file as an exception or temporarily deactivate virus scans during the installation process) and of the customer's antivirus

policy.
In cases where the file size or the checksum differs, or where other files than "lib\PortOpen.exe" are identified as potentially malicious: raise a ticket for further clarification.
Note that Unify's Secure SW development and release process includes continuous virus scanning throughout all involved instances (from software developers' workstations, software production servers to software download servers) to prevent from any malware ever being delivered unintentionally to our customers.

References

n.a.

Revision History

2016-02-05: Initial release

2016-09-29: Update 01

- Informational update only: the relevant file that produced the false positive virus alert was removed from the OpenScape Accounting Management installation package in V2 R0.11.0

Advisory ID: OBSO-1602-01 (a=135), 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

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.