Security Advisory Report - OBSO-1703-01

Wikileaks: CIA Hack of Siemens/ Unify telephones

Creation Date: 2017-03-10
Last Update: 2017-03-10

Summary

Wikileaks published a way to establish access to a Siemens/ Unify OpenStage 15 phone.

https://wikileaks.org/ciav7p1/cms/page_2621481.html

This is only possible if the phone has a default Admin password.

Vulnerability Details

The document "Vault 7: CIA Hacking Tools Revealed" describes how an OpenStage 15 phone can be manipulated via a ssh access.

TFTP is used to upload tshd (tiny shell)

Persistent root shell access is established.

The article is from June 2013. The phone had version V2 R0.92.0

Unify phones are not affected, since the access was established with an ssh connection and ssh is deactivated by default.
A valid Admin password is required to activate ssh.

The customer is advised via security checklist to set an individual, customer-specific Admin password of his choice.

The vulnerabilities documented here can be classified as not critical, since some important changes have been made to Unify phones since 2013 (release date of the mentioned version).
In summary, it can be said that if a customer has the latest version of the phones in use and keeps to the current security checklist, he is very well protected against the vulnerabilities described in the document.

Unify Software and Solutions GmbH & Co. KG, does its best keep to its products safe.
Examples:

- ROOT access has been removed from the SSH functions. SSH only works with restricted admin rights.
- Penetration tests and Theoretical security Assessments are regularly conducted to eliminate vulnerabilities before the products are used by the customer.
- With each new major and minor version, the security checklist is updated and republished.
  In this checklist we state, for example, that the default admin password should be changed.
- Our telephones are regularly checked for security vulnerabilities and critical weaknesses are published here and of course solved as quickly as possible:

https://www.unify.com/security/advisories

https://networks.unify.com/security/advisories/Security_Policy_Vulnerability_Intelligence_Process.pdf

Affected Products

All Unify OpenStage and OpenScape SIP and HFA Desk Phones have ssh access, but are not affected as mentioned above.
TDM, DECT and WLAN phones do not support ssh.

Recommended Actions

The documented security flaw is solved by Unify, by permanently disabling root access with SSH and documenting all security measurements in the

security checklist.
The activities described in the WikiLeaks document are only feasible if the phone still has a default password.
In the WikiLeaks document we cannot find a vulnerability to crack the admin password, so as soon as the admin has supplied the phones with a secure password this security flaw becomes obsolete.

SSH access on phones is disabled by default. It must be enabled via the GUI in the Admin menu.
The Admin GUI can only be reached with knowledge of the Admin password.
In the security checklist the customer is advised to change the default Admin password to a customer-specific password of his choice.

The security checklist for CP phones clearly states:
SSH Interface
The Secure Shell interface is reserved for technical specialists. It is deactivated by default and can be enabled by the Admin user via WBM or DLS for each access.
It is enabled for a limited period of time only, and a password is set for the access.
A different password should be used for each access.
To prevent all access via secure shell the secure shell allowed can be disabled.
This is done via DLS.

References

https://wikileaks.org/ciav7p1/cms/page_2621481.html

Revision History

First draft 2017-03-09

Update 2017-03-10

Advisory ID: OBSO-1703-01 (a=160), status: general 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