Security Advisory Report - OBSO-1010-03

Impact of the Stuxnet worm to Unify systems

Creation Date: 2010-10-25
Last Update: 2013-11-08

Summary

Customers are asking whether our (Unify) systems are potentially vulnerable to the Stuxnet worm.

This Security Advisory discusses the impacts of the worm for customers using Unify products and systems.

Vulnerability Details

The Stuxnet worm uses various known vulnerabilities in Microsoft Windows operating systems to infect computers, primarily via the USB interface. The Windows computers are not the target of the worm. Instead, it uses them to distribute itself to computers where the Siemens AG controller software SIMATIC WinCC is installed. The final target of the worm are Programmable Logic Controllers (PLC) managed by the WinCC software.

The Stuxnet worm is doing currently nothing malicious on Windows computers if no PLC/WinCC system is found.

Since the time of its writing (which is estimated in 2008/2009), the worm used a number of zero-day exploits (where a patch or countermeasure did not exist yet) in the Windows operating system to distribute itself to Windows computers worldwide. Meanwhile for all exploits that are known to be used by Stuxnet, appropriate security updates are provided by Microsoft.

Currently there is no indication that, besides Windows computers and PLC software, the worm tries to infect other systems for distribution and/or attacks. This includes any Linux or VxWorks based systems provided by Unify.

As part of the Vulnerability Intelligence Process, the OpenScape Baseline Security Office is continuously monitoring updated information regarding the Stuxnet worm and its variants. In case of significant changes to the current evaluation, we will inform our customers by an update of this Security Advisory.

Affected Products

As of today, no products provided by Unify are known to be affected.

Furthermore, products and applications provided by Unify do not contain and do not rely on PLC/WinCC software.

Recommended Actions

No specific actions for telecommunication systems provided by Unify are required.

All Windows-based applications provided by Unify, are conformant with the relevant policies regarding support of Operating System updates and Antivirus software.

Therefore, to avoid that the Stuxnet worm uses Unify application servers for further distribution, it is recommended to apply appropriate updates and install antivirus software according to these policies:

- wiki.unify.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf
- wiki.unify.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

References

- https://secure.wikimedia.org/wikipedia/en/wiki/Stuxnet
- www.schneier.com/blog/archives/2010/10/stuxnet.html
- www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Unify-specific references, as already listed in the advisory text above:

- wiki.unify.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf
- wiki.unify.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

Revision History

2010-10-25 Initial release
2010-10-27 Update release with minor additional information
2013-11-08 Rereleased under the Unify brand (formerly Siemens Enterprise Communications)

Advisory ID: OBSO-1010-03 (a=6), 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.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.