Primary Stuxnet Advisory | CISA

Published: 2018-09-06 · Archived: 2026-04-02 12:36:20 UTC

OVERVIEW

ICS-CERT has been actively investigating and reporting on the Stuxnet vulnerability. To date, ICS-CERT has released ICSA-10-201-01 - Malware Targeting Siemens Control Software (including Updates B & C) and ICSA-10-238-01 - Stuxnet Mitigations (including Update B).

Stuxnet uses four zero-day exploits (two of which have been patched) and takes advantage of a vulnerability also exploited by Conficker, which has been documented in Microsoft Security Bulletin MS-08-067.Microsoft Security Bulletin, http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx, website last accessed September 28, 2010. The known methods of propagation include infected USB devices, network shares, STEP 7 Project files, WinCC database files, and the print spooler vulnerability addressed by MS-10-061.Microsoft Security Bulletin, http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx, website last accessed September 28, 2010. The malware can be updated through a command and control infrastructure as well as peer-to-peer communication using the Remote Procedure Call (RPC) protocol.

The malware also interacts with Siemens SIMATIC WinCC or SIMATIC STEP 7 software. Exact software versions and configurations that may be affected are still being analyzed jointly by ICS-CERT and Siemens. We have listed the following indicators for use in detecting this malware.

PRIMARY MALWARE INDICATORS

INDICATOR LIST OVERVIEW

The following indicator list was developed by ICS-CERT and will be useful in detecting malicious files in systems infected with Stuxnet. Tests were performed on two systems. One system was a new installation of Windows XP SP3 that was subsequently infected with Stuxnet. The other machine was the same Windows configuration but also included Siemens WinCC and STEP 7 software installations. Based on these tests, ICS-CERT has determined that these indicators fall into two groups. Some indicators appear on systems whether or not they have Siemens WinCC/STEP 7 installed, and the others only appear on systems with WinCC/STEP 7 installed.

INFECTED MACHINES WITH/WITHOUT WINCC/STEP 7 INSTALLED

Filename and Path	Hash
WINDOWS\inf\mdmeric3.PNF	b834ebeb777ea07fb6aab6bf35cdf07f
WINDOWS\inf\oem6C.PNF	Hash may vary

WINDOWS\inf\oem7A.PNF	ad19fbaa55e8ad585a97bbcddcde59d4
WINDOWS\inf\mdmcpq3.PNF	Hash may vary
WINDOWS\system32\drivers\mrxcls.sys	f8153747bae8b4ae48837ee17172151e
WINDOWS\system32\drivers\mrxnet.sys	cc1db5360109de3b857654297d262ca1

INFECTED MACHINES WITH WINCC/STEP 7 INSTALLED

Filename and Path	Hash
WINDOWS\system32\s7otbxdx.dll (malicious file has the same name as the original legitimate STEP 7 file)	7a4e2d2638a454442efb95f23df391a1
WINDOWS\system32\s7otbxsx.dll (this is the original legitimate STEP 7 file which has been renamed by the malware)	5b855cff1dba22ca12d4b70b43927db7

The following files may be found in WinCC/STEP7 Project directories.

Filename and Path	Hash
\GraCS\cc_alg.sav	ad19fbaa55e8ad585a97bbcddcde59d4
\GraCS\cc_tag.sav	Hash may vary
\GraCS\cc_tlg7.sav	d102bdad06b27616babe442e14461059
\GraCS\db_log.sav	b834ebeb777ea07fb6aab6bf35cdf07f

In infected projects, the malicious *.sav files are stored in the GraCS subdirectory within a project's root directory. This can occur in compressed or zipped project files. It appears that the malware specifically looks for demo projects commonly installed as part of the WinCC software. If any of these malicious *.sav files are found, it is likely that the malware has injected malicious stored procedures into one or more of the project's database files. If any of these malicious *.sav files are detected, please contact ICS-CERT for further assistance.

MITIGATION

For information regarding Stuxnet mitigations, please refer to ICSA-10-238-01B – Stuxnet Mitigations.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds

organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.
