ICS-CERT ADVISORY

ICSA-10-201-01C—USB MALWARE TARGETING SIEMENS CONTROL SOFTWARE

UPDATE C

August 02, 2010

OVERVIEW

VirusBlokAda, an antivirus vendor based in Belarus, announced[a] the discovery of malware that uses a zero-day vulnerability in Microsoft Windows processing of shortcut files. The malware uses this zero-day vulnerability and exploits systems after users open a USB drive with a file manager capable of displaying icons (like Windows Explorer). US-CERT has released a Vulnerability Note[b] detailing the vulnerability and suggested workarounds. Microsoft has also released a Security Advisory (2286198)[c] detailing the previously unknown vulnerability.

ICS-CERT has confirmed the malware installs a Trojan that interacts with installed SIMATIC WinCC or SIMATIC Siemens STEP 7 software and then makes queries to any discovered SIMATIC databases. The full capabilities of the malware and intent or results of the queries are not yet known.

ICS-CERT is coordinating with Siemens CERT, CERT/CC, Microsoft, and other groups both domestically and internationally to share analysis and information.

AFFECTED SYSTEMS

Microsoft reports that the zero-day vulnerability affects the following versions of Windows:

- Windows XP Service Pack 3
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 1 and Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2

a. VirusBlokAda, http://www.anti-virus.by/en/tempo.shtml, website last accessed July 15, 2010.

b. Vulnerability Note, http://www.kb.cert.org/vuls/id/940193, website last accessed July 16, 2010.

c. Microsoft Security Advisory, http://www.microsoft.com/technet/security/advisory/2286198.mspx, website last accessed July 19, 2010.

- Windows 7 for 32-bit Systems
- Windows 7 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems
- Windows Server 2008 R2 for Itanium-based Systems.

There are also unconfirmed reports Windows 2000 and Windows XP SP2 are susceptible to this zero-day vulnerability.

The malware also appears to interact with SIMATIC WinCC or SIMATIC Siemens STEP 7 software. Exact software versions and configurations that may be affected are still being analyzed jointly by ICS-CERT and Siemens CERT.

IMPACT

The actual impact to control environments is not yet known. ICS-CERT is currently evaluating the malware to determine the potential affects that it could have on control system environments.

On July 18, 2010, proof-of-concept exploit code for the zero-day Windows vulnerability was publicly released.

BACKGROUND

SIMATIC WinCC HMI is a scalable process-visualization system for monitoring automated processes.

SIMATIC STEP 7 is engineering software used in the programming and configuration of SIMATIC programmable controllers.

These products are widely used in many critical infrastructure sectors.

MALWARE CHARACTERIZATION

MALWARE DETAILS

The malware appears to launch when a storage device is viewed using a file manager such as Windows Explorer. Because the malware exploits a zero-day vulnerability in the way that Windows processes shortcut files, the malware is able to execute without using the AutoRun feature.

Shortcut files are Windows files that link easy-to-recognize icons to specific executable programs, and are typically placed on the user's Desktop or Start Menu. A shortcut will not execute until a user clicks on its icon. While Microsoft's advisory indicates user's need to click an icon for the vulnerability to be executed, VirusBlokAda reports these malicious shortcut files are capable of executing automatically (without user interaction) if accessed by Windows Explorer.

This vulnerability is most likely to be exploited through removable drives. For systems that have AutoPlay disabled, customers would need to manually browse to the root folder of the removable disk in order for the vulnerability to be exploited. For Windows 7 systems, AutoPlay functionality for removable disks is automatically disabled.

Based on current reporting,[d] the malware drops and executes two driver files: **mrxnet.sys** and **mrxcls.sys**. The mrxnet.sys driver works as a file system filter driver, and mrxcls.sys is used to inject malicious code. These files are placed in the %SystemRoot%\System32\drivers directory. The drivers were signed with the apparent digital signature of Realtek Semiconductor Corporation. No warning is displayed in Windows when the drivers are installed, even though the certificate used to sign the files expired in June 2010. VeriSign has revoked the certificate used to sign the malware. The two drivers are used to inject code into system processes to hide themselves. Using this method, the malware files are not visible on an infected USB storage device.

Currently, some analysis has been performed and published on the Siemens-specific capabilities of the malware. ICS-CERT has confirmed the database query strings do, in fact, reference WinCC database tables containing Input/Output tags. As more details become available and analysis is verified, ICS-CERT will publish updates to this advisory.

--------- Begin Update B- 1 of 2 --------

ICS-CERT has found indications that the malware checks for installations of antivirus software. System owners using antivirus software should ensure the software is working properly, because these findings may indicate the malware is capable of disabling antivirus functionality.

Symantec has also performed some in-depth analysis of the Stuxnet malware files.[e] This information has not been independently verified by ICS-CERT but is included for reference.

CALLBACK DOMAINS/COMMAND & CONTROL

Independent analysis from multiple sources[f,g,h,i] has identified the following domains as command and control domains associated with the malware. ICS-CERT has not independently verified these findings, but calls to these domains may indicate a compromise.

- mypremierfutbol.com
- todaysfutbol.com.

d. VirusBlokAda, http://www.wilderssecurity.com/attachment.php?attachmentid=219888&d=1279012965, website last accessed July 15, 2010.

e. Symantec, http://www.symantec.com/connect/blogs/distilling-w32stuxnet-components, http://www.symantec.com/connect/blogs/w32stuxnet-variants, http://www.symantec.com/connect/blogs/w32stuxnet-network-operations, http://www.symantec.com/connect/blogs/w32stuxnet-network-information, http://www.symantec.com/connect/blogs/w32stuxnet-installation-details, last accessed July 29, 2010.

f. Zscaler Research, http://research.zscaler.com/2010/07/lnk-cve-2010-2568-stuxnet-incident.html, last accessed July 22, 2010.

g. Siemens Forum, http://www.automation.siemens.com/WW/forum/guests/PostShow.aspx?PageIndex=1&PostID=225893&Language=en last accessed July 22, 2010.

h. CERT-In, http://www.cert-in.org.in/virus/Stuxnet_Rootkit.htm, last accessed July 22, 2010.

i. TrendMicro, http://threatinfo.trendmicro.com/vinfo/web_attacks/Worm%20Propagates%20via%20Windows%20Shortcut%20Vulnerability%20Exploit.html, last accessed July 22, 2010.

In addition, some sources are reporting that HTTP requests with the following content may be indicative of a compromised host:

- "index.php?data=66a96e28"

--------- End Update B- 1 of 2 --------

INSTALLED FILES[j]

C:\WINDOWS\system32\drivers\mrxnet.sys
C:\WINDOWS\system32\drivers\mrxcls.sys
C:\WINDOWS\inf\oem7A.PNF
C:\WINDOWS\inf\oem6C.PNF
C:\WINDOWS\inf\mdmeric3.PNF
C:\WINDOWS\inf\mdmcpq3.PNF

MITIGATION

Microsoft's Security Advisory (2286198)[k] provides workarounds to mitigate this previously unknown vulnerability being exploited by this malware:

- Disable the displaying of icons for shortcuts
- Disable the WebClient service.

--------- Begin Update A --------

Microsoft has released an updated advisory that includes:

- Information on an additional attack vector identified through the use of PIF files, which are very similar to LNK shortcuts.
- Updated workarounds to reflect that the IconHandler also needs to be edited.
- A new Fix It tool, which allows administrators and users to more easily deploy the workaround.
- A workaround to block downloading of LNK and PIF files from the internet. These files cannot be renamed, but any blocking solution should take into account the WebDAV protocol, if the WebDAV client has not already been disabled.
- Clarification of some of the possible attack vectors, including the use of an embedded shortcut in an Office document, or the use of a web browser to browse malicious content.

Other suggested workarounds to help reduce the risks to this and other vulnerabilities include:

- Disable AutoRun as described in Microsoft Support Article 967715
- Implement the principle of least privilege as defined in the Microsoft TechNet Library

j. VirusBlokAda , http://www.wilderssecurity.com/attachment.php?attachmentid=219888&d=1279012965, website last accessed July 15, 2010.
k. Microsoft Security Advisory, http://www.microsoft.com/technet/security/advisory/2286198.mspx, website last accessed July 21, 2010.

- Maintain up-to-date antivirus software.

Siemens has also released an advisory[l] to address questions surrounding this issue. Siemens has indicated that they have received one notification of an infection to an organization in Germany. The damage, if any, is unknown at this time.

--------- Begin Update C – Part 1 of 2 ----------

Siemens indicates four customers have been infected worldwide with no impact to production.[m]

---------- End Update C – Part 1 of 2 ----------

Antivirus vendors[n,o] have indicated the presence of a second Stuxnet variant. Most reports indicate the new rootkit driver is very similar to previously observed samples. The main difference has been the use of a certificate from JMicron Technology Corporation to digitally sign the driver.

---------- End Update A ---------

--------- Begin Update B-2 of 2 -------

SIEMENS SECURITY UPDATE

Siemens has released a Security Update: SIMATIC_Security_Update_20100722.exe, which is available on their support website: http://support.automation.siemens.com/WW/view/en/43876783.

According to Siemens, the SIMATIC update accomplishes the following:

- Modifies the registry settings according to Microsoft's Security Advisory[k] Version 1.2.
- Adapts the SQL Server settings to the latest security settings. This step will make for stricter authentication controls.

Installing this SIMATIC update will replace all Siemens system icons with standard Windows icons. Siemens recommends meaningful names be assigned to desktop and Windows Start menu links so they may be easily recognized after the update.

In addition, Siemens product support has provided a link to download a copy of Trend Micro System Cleaner (Sysclean) to assist users in detecting/cleaning infected systems.

---------- End Update B-2 of 2 -------- Owners and operators should exercise caution and consult their control systems vendor prior to making any changes or using antivirus software. Proper impact analysis and testing should always be conducted prior to making any changes to control systems. Siemens CERT

l. Siemens, http://support.automation.siemens.com/WW/view/en/43876783, website last accessed July 22, 2010.
m. Siemens, http://support.automation.siemens.com/WW/view/en/43876783, website last accessed July 22, 2010.
n. F-Secure, http://www.f-secure.com/weblog/archives/00001993.html, website last accessed July 21, 2010.
o. Jeremy Kirk, http://www.infoworld.com/d/security-central/second-variant-stuxnet-worm-strikes-944?source=rss_infoworld_news, website last accessed July 21, 2010.

has indicated that they are performing testing on the mitigations to determine their possible effects on control systems.

ICS-CERT reminds users to exercise caution when using USB drives. For more information on best practices and removable media, see the ICS-CERT Control Systems Analysis Report "USB Drives Commonly Used As An Attack Vector Against Critical Infrastructure."[p]

Malware samples have been provided to the antivirus vendor community. ICS-CERT recommends consulting your antivirus and control systems vendor before scanning systems with current antivirus software. The malware is identified by some antivirus vendors as the following:

- DrWeb: Trojan.Stuxnet.1
- ESET: Win32/Stuxnet.A
- F-Secure: Exploit:W32/WormLink.A
- Ikarus: Trojan-Dropper.Win32.Stuxnet
- Kaspersky: Trojan-Dropper.Win32.Stuxnet.a
- Mcafee: Stuxnet
- Microsoft: TrojanDropper:Win32/Stuxnet.A
- Norman: W32/Stuxnet.C
- Panda: Trj/CI.A
- Sophos: Troj/Stuxnet-A
- TrendMicro: WORM_STUXNET.A.

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.

--------- Begin Update C – Part 2 of 2 ----------

Microsoft has released an out-of-band security bulletin on Monday, August 2, 2010[q] to address the vulnerability used by the Stuxnet malware to infect systems

The Microsoft bulletin addresses a security vulnerability that exists in all supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. ICS-CERT recommends that all control systems operations personnel work with their vendor to assess potential impacts before implementing this new fix. ICS-CERT also recommends coordinating with your vendor to determine if the operating system provided in your control systems installation is affected by this vulnerability and if a fix is available.

---------- End Update C – Part 2 of 2 ----------

p. ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf, website last accessed July 15, 2010.

q. http://www.microsoft.com/technet/security/bulletin/ms10-aug.mspx

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting:
www.ics-cert.org