ICS-CERT ADVISORY

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

July 20, 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 utilizes 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. ICS-CERT will provide updates as needed.

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

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

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

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

- Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2
- 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 that Windows 2000 and Windows XP SP2 are also 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 USB 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 that 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.

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

INSTALLED FILES[e]

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)[f] provides workarounds to mitigate this previously unknown vulnerability being exploited by this malware:

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

Control system owners and operators should consult the Microsoft Advisory (2286198)[f] for details. Owners and operators should exercise caution however, and consult their control systems vendor prior to making any changes. Proper impact analysis and testing should always be conducted prior to making any changes to control systems. Siemens CERT 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[g]".

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 anti-virus vendors as the following:

- Mcafee: Stuxnet
- Kaspersky: Trojan-Dropper.Win32.Stuxnet.a
- TrendMicro: WORM_STUXNET.A

e. VirusBlokAda , http://www.wilderssecurity.com/attachment.php?attachmentid=219888&d=1279012965, website last visited July 15, 2010.
f. Microsoft Security Advisory, http://www.microsoft.com/technet/security/advisory/2286198.mspx, website last visited July 19, 2010.
g. ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf, website last visited July 15, 2010.

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

As details of the malware become better known, further mitigation recommendations will be published.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

CONTACT ICS-CERT:

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

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