

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

7/17/2010

SUBJECT:

Vulnerability in Windows Shell Could Allow Automatic File Execution

OVERVIEW:

A vulnerability has been discovered in Windows Shell, component of Microsoft Windows Operating System, that could allow automatic file execution. Specifically this vulnerability exists because Microsoft Windows incorrectly parses shortcuts (LNK files) in such a way that malicious code may be executed when the user views the displayed icon of a specially crafted shortcut. Successful exploitation may result in an attacker gaining at least the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It has been confirmed that this vulnerability is being exploited in limited targeted attacks, however, we should anticipate more widespread exploitation in the short term.

There is currently no patch available for this vulnerability.

SYSTEMS AFFECTED:

- * Windows XP
- * Windows Vista
- * Windows 7
- * Windows Server 2003
- * Windows Server 2008

RISK:

Government:

- * Large and medium government entities: High
- * Small government entities: High

Businesses:

- * Large and medium business entities: High
- * Small business entities: High

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Windows Shell in the way it processes shortcut 'LNK' files that could allow automatic file execution. Exploitation may occur when the user views the displayed icon of a specially crafted shortcut. No user interaction is required other than viewing a folder while

the specially crafted shortcut is displayed. Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Current reports indicate that this vulnerability is being exploited with USB and other removable media. It is possible for this vulnerability to be exploited through network shares.

This vulnerability is being exploited in limited targeted attacks and currently being detected as W32.temphid (Symantec), Troj/Stuxnet-A (Sophos), or Rootkit.TmpHider (VirusBlokAda). The malware created to exploit this vulnerability appears to be targeting Siemens WinCC SCADA systems at this time according to independent researcher Frank Boldewin.

It should be noted that having AutoPlay disabled will prevent automatic file execution on removable disks. However, the attack could still be successful if the user browses to the root folder of the removable disk. Windows 7 has AutoPlay functionality for removable disks disabled by default.

There is currently no patch available for this vulnerability.

Microsoft has not released a patch for this vulnerability at this time, and is currently provided a workaround for disabling the displaying of icons for shortcuts and disabling the use of WebDAV which are known current attack vectors.

To disable the displaying of icons perform the following steps:

1. Click Start, click Run, type Regedit in the Open box, and then click OK
2. Locate and then click the following registry key:
HKEY_CLASSES_ROOT\lnkfile\shellex\IconHandler
3. Select the value (Default) on the right hand window in the Registry Editor. Press Enter to edit the value of the key. Remove the value, so that the value is blank, and press Enter.
4. Restart explorer.exe or restart the computer.

To disable the WebClient service perform the following steps:

1. Click Start, click Run, type Services.msc and then click OK.
2. Right-click WebClient service and select Properties.
3. Change the Startup type to Disabled. If the service is running, click Stop.
4. Click OK and exit the management application.

RECOMMENDATIONS:

The following actions should be taken:

- * Ensure that all anti-virus software is up to date with the latest signatures.
- * Blocking outbound SMB connections on the perimeter firewall will reduce the risk of remote exploitation using file shares.
- * Consider disabling the displaying of icons for shortcuts
- * Consider disabling the WebClient service where possible
- * Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- * Establish policies for the use of removable media on all enterprise and control system networks.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/41732>

US-CERT:

<http://www.kb.cert.org/vuls/id/940193>

Krebs on Security Blog:

<http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>

F-Secure:

<http://www.f-secure.com/weblog/archives/00001986.html>

http://www.f-secure.com/weblog/archives/new_rootkit_en.pdf

VirusBlokAda:

<http://www.anti-virus.by/en/tempo.shtml>

Microsoft:

<http://support.microsoft.com/kb/2286198>

<http://www.microsoft.com/technet/security/advisory/2286198.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568>