Vulnerability Advisory

Name	Skype - URI Handler Input Validation
Vendor Website	http://www.skype.com
Date Released	March 11th, 2010
Affected Software	Skype for Windows: All releases prior to 4.2.0.1.55 (v4.2 hotfix #1)
Researcher	Paul Craig – Paul.Craig@security-assessment.com

Description

The Windows Skype client implements two URI handlers, Skype: and Skype-Plugin. Both handlers allow for easy browser integration and are supported by all modern browsers. When a Skype link is clicked, the Skype.exe process is spawned with the /URI: command argument, followed by the user specified phone number or contact name.
For example, clicking the link: Skype:PaulCraig will spawn the process **Skype.exe "/URI:Skype:paulcraig"**

Due to a flaw in the current user input validation performed by Skype, it is possible to append additional command line arguments which are subsequently processed during the launch of Skype.exe.

In 2006 colleague Brett Moore, discovered a similar vulnerability in Skype which led to certain security restrictions being enforced when using the Skype: URI handler. Brett's exploit at the time involved including additional command line arguments to the Skype.exe process which would send a file to a remote user when a Skype link was clicked. Changes were made to Skype to remove available command line arguments when the /URI argument is present.

Although many of the useful arguments have been disallowed (such as sending a file to a remote user) Security-Assessment.com found that the /Datapath argument can be included and directed to a remote SMB share directly through the Skype URI handler. The *Datapath* argument specifies where the Skype configuration files and security policy is kept. Specifying a *Datapath* argument will override any local security policy defined in the Windows registry.

A remote user is capable of crafting a link that when clicked, will spawn Skype.exe on a client using a *Datapath* location which is present on a remote SMB share. The Skype client will load any configuration or security policy present and save the users Skype account information to the remote share.

This allows a remote user to control the Skype configuration and security policy of the local client instance of Skype. Settings such as a remote proxy can be defined, which could be used to Man In the Middle Skype communications.
Security-Assessment.com also found that the contents of another user's *Datapath* contained a wealth of private information and call history associated with the user.

Exploitation

Exploitation occurs when the victim clicks a malformed Skype link in Internet Explorer (6,7 or 8) or Chrome. The exploit originates from a failure to sanitise raw binary content correctly, and the ability of ShellExecute() to permit URIs which contain raw binary values.

Security-Assessment.com found that the Skype: URI handler permits the double quote and forward slash (" and /) characters within a Skype URI, but does not permit any whitespace characters (such as space, %20, +) to be included. This essentially protects Skype from a user inserting additional command line arguments directly within the Skype: link, as a command line argument separator character (whitespace) cannot be included.

However, the use of a raw binary byte is permitted by Skype and the byte is subsequently treated as a whitespace value when parsing Skype.exe command line arguments. This provides a whitespace character, without being a traditional whitespace. This method of whitespace character injection can be used to include additional command line arguments to the Skype.exe process.

The example below illustrates this.

Click Me
Where 0x01 represents the RAW binary byte value 0x01.

This URL will result in the Skype configuration being retrieved from the remote host 'remotehost'. Once a user has authenticated using Skype, the Skype client will download their chat history and call logs to the remote share.

Other arguments such as /username and /password can also be included using the same method of whitespace injection. This is illustrated below.

Click Me

The bytes 0x01-0x07 were found to function as a replacement for a whitespace character.

Recommendations

Skype have created a fix for this vulnerability which has been included as part of Skype v4.2 hotfix #1. Security-Assessment.com recommends all users of Skype upgrade to the latest version as soon as possible. For more information on the new release of Skype please refer to the release notes:

http://share.skype.com/sites/garage/2010/03/10/ReleaseNotes_4.2.0.155.pdf

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognized companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognized through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web: www.security-assessment.com
Email: info@security-assessment.com