

Vulnerability Advisory

Name	Skype - URI Handler Command Switch Parsing
Vendor Website	http://www.skype.com
Date Released	May 22, 2006
Affected Software	Skype for Windows: All releases prior to and including 2.0.*.104 Release 2.5.*.0 to and including 2.5.*.78
Researcher	Brett Moore brett.moore@security-assessment.com

Description

During the typical installation of the Windows Skype client, several URI handlers are installed. This allows for easy access to the Skype client through various URI types.

Due to a flaw in the handling of one of these types, it is possible to include additional command line switches to be passed to the Skype client. One of these switches will initiate a file transfer, sending the specified file to an arbitrary Skype user.

Exploitation

Exploitation occurs when the victim opens the exploit URI in Internet Explorer. This requires the victim to visit a website under the attackers control, or to be convinced into opening a malicious HTML page. Clicking on a link is not required, as this action can be automated in various ways using scripting language.

For the attack to be successful the attacker must know the location of the requested file on the victims machine. One common target file would be the victims Skype configuration file.

For the file transfer to succeed the attacker must have authorized the victim, which can be done by adding the victim to the attackers contact list. This does not require any authorisation from the victim Skype user.

Other Skype command line switches could also be exploited to manipulate or obtain the Skype users credentials, under similar situations.

Solution

Install the vendor supplied upgrade;
<http://www.skype.com/security/skype-sb-2006-001.html>

About Security-Assessment.com

Security-Assessment.com is New Zealand's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout Australasia. Our clients range from small businesses to some of the largest globally recognized companies. Security-Assessment.com has no vendor relationships and positions itself as the only independent security assurance provider in New Zealand.

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

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093