

LATEST NEWS

Telecom seeks relief on three-way split

Industry slams Telecom's request for relief

We're ready to go: Vector

Mobile Termination Rates will be regulated | 4

Blackbox cracks the code

At the 2degrees 3G launch | 1

Kiwi security expert finds flaw in Skype

The flaw could potentially allow an attacker to steal confidential files

BY ULRIKA HEDQUIST AND JUHA SAARINEN | AUCKLAND | TUESDAY, 6 JUNE, 2006

EMAIL PRINT

A security flaw in Skype's peer-to-peer VoIP software has been closed, thanks to diligent work by a Kiwi security expert.

Auckland-based Brett Moore, CTO of Australian, independent security company Security-Assessment.com, uncovered the flaw in Skype's software. Skype is now advising users to upgrade to its latest version to fix the bug.

Moore says that the type of vulnerability found in Skype is fairly common with applications that interact with internet browsers.

"We have previously discovered this type of vulnerability in two separate programs and there are public releases of similar issues in other programs," he says.

The security flaw manifests itself through the way Skype handles Uniform Resource Identifiers (URIs) that point to names or addresses referring to resources.

Security-Assessment.com discovered that with one type of URI handler installed by Skype it was possible to include additional command-line switches. One such switch will set up a file transfer session that will allow data written to the local hard disk to be sent to another Skype user.

For an attacker to successfully exploit the flaw he must know the exact name and location of the file he wants to transfer on the victim's computer. The attacker must also authorise the victim, Security-Assessment.com says. This is easily done, with the attacker simply adding the victim to his contact list.

There are further URI handler flaws in Skype, Security-Assessment.com says. Other command-line switches could be exploited to manipulate or obtain victims' Skype user credentials.

Security-Assessment.com regularly performs application testing for its customers or as part of its own R&D, says Moore.

"In this case, we were reviewing Skype as part of a larger VoIP research programme. Often we will notice what appears to be the potential for a vulnerability and investigate further."

Moore says that a targeted attack is required to exploit this particular vulnerability.

"The person to be exploited must be specifically selected and they must be convinced to browse to a web page or click on a hyperlink," he says. "While there are certain mitigating factors involved in a successful attack, the potential is there for an attacker to steal confidential files, including the user's Skype configuration."

Theft of the Skype configuration could lead to further attacks such as ID theft, or listening in on users' conversations, he says.

"The best solution is to install the vendor-supplied update," Moore says.

"As always, users should be aware of malicious emails and email attachments."

When discovering security flaws the company works directly with the vendor involved to help secure their software, Moore says.

Unlimited
INVESTMENT CHALLENGE
DO YOU NEED CAPITAL TO GROW?
Then take the **Unlimited Investment Challenge**.
CLICK HERE FOR MORE INFORMATION

READ	COMMENTED	EMAILED	SHARED
<ul style="list-style-type: none"> "UFB is a piece of ..." Internet account ban no worse than driving penalty Datacom chief dies suddenly iFiasco At the 2degrees 3G launch Chorus2 can deliver on urban and rural fibre 			

SUBSCRIBE



Computerworld is New Zealand's only specialised information systems fortnightly. **Subscribe now** for \$97.50 (24 issues) and save more than 37% off the cover price!



SIGN UP



Get the latest news from **Computerworld** delivered via email. **Sign up now**

POPULAR EVENTS

SUSTAINABLE 60 AWARDS	The Sustainable 60 Awards Entries open now. Click here for more details
Unlimited INVESTMENT CHALLENGE	Unlimited Investment Challenge 2010 Entries open now. Click here for more details
SUSTAINABLE 60 WORKSHOPS	The Sustainable 60 Workshops Dates confirmed Click here for more details

SPONSORED LINKS

COMPUTERWORLD	Local and International news Enterprise ICT must know info Subscribe today
PC WORLD \$599!	NZ's most trusted tech advice Free NZ Delivery Subscribe today

Telecom Broadband Offer
Double what you love doing online Conditions apply.
Sign up now
www.telecom.co.nz/broadband-offer

Telecom Total Office
Think you won't get a better deal on landline+broadband? Think again.
www.telecombusinesshub.co.nz

Fly with Orcon Internet
Switch to Orcon Broadband Today & You'll Get 60 Airpoints Dollars!
www.orcon.net.nz/special-offer

Careers - NZ's #1 Site
SEEK has over 10,000 new jobs Get Jobs emailed daily.
SEEK.co.nz

“Skype was very happy to work with us on this issue. They phoned me shortly after receiving our security report and kept me up to date with their progress,” he says.

“During the patch development they called me to discuss further details, and sent me a pre-release install to verify that they had fixed the problem.”

Moore was a little surprised to find the bug in Skype because it has already undergone independent security reviews, and also because of the large numbers of users.

SHARE THIS STORY WITH:

 EMAIL
 PRINT
 



MOST POPULAR STORIES FROM FAIRFAX BUSINESS MEDIA GROUP WEBSITES



- Leading through massive change
- Easing the information management headache
- Exit interview: Kevin Ackhurst of Microsoft NZ
- Yours leadership portfolio: The view from C-level
- How to sack your IT supplier



- Breathe new life into your laptop's battery
- Kiwis may be eligible for iPhone 4 refunds
- Press F1: Where's the power?
- Microsoft exec mocks iPhone 4, dubs it Apple's Vista
- Apple confirms iPhone 4 refund policy
- 2 degrees launches 3G services



- The habits of highly ineffective resellers
- iPhone 4 launch delayed
- SAP warms to open source
- Government hardware deals in the offing
- Citrix tops VMware in desktop virtualisation, again



- Change agents
- Creating value for NZ Inc through cleantech
- Customer complaints matter
- Sun sets on the Bill Day Show
- Productivity's last great hope at hope

© Fairfax Media Business Group
Fairfax New Zealand Limited, 2010

FairfaxBG - Computerworld - PC World - Reseller News - CIO - Unlimited - actv8

Email Webmaster - Contact Fairfax Media Business Group - Subscribe Online - Advertise With Us - Privacy Policy