

[NT] Skype skype4com URI Handler Remote Heap Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00017.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 10 Dec 2007 14:42:08 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Skype skype4com URI Handler Remote Heap Corruption Vulnerability

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Skype. User interaction is required to exploit this vulnerability in that the target must visit a malicious page.

DETAILS

Vulnerable Systems:

- * Skype versions prior to 3.6 GOLD

The specific flaw exists within the 'skype4com' URI handler created by Skype during installation. When processing short string values through this handler an exploitable memory corruption may occur which can result in arbitrary code execution under the context of the current user.

Vendor Response:

Skype has corrected this issue as of 11/15/2007. All clients updated or installed as of that date are patched to this issue.

Disclosure Timeline:

[NT] Skype skype4com URI Handler Remote Heap Corruption Vulnerability

2007.11.02 – Vulnerability reported to vendor
2007.12.06 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5989>>
CVE-2007-5989

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
The Zero Day Initiative (ZDI).

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-07-070.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-070.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.