

uuuppz.com – Advisory 002 – mIRC \$asctime overflow

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0070.html>

From: James Martin (fulldisclose@UUUPPZ.COM)

Date: 08/27/02

Date: Tue, 27 Aug 2002 14:58:50 +0100
From: James Martin <fulldisclose@UUUPPZ.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

General Info

Researched by: James Martin
Full advisory: <http://www.uuuppz.com/research/adv-002-mirc.htm>
Exploit: Proof of concept code available at above URL.

Product: mIRC
Website: <http://www.mirc.com>
Version: V6.00, V6.01, V6.02.
Fix: Download mIRC 6.03 from <http://www.mirc.com>
Please do not download from unofficial sites, as you may download a trojaned version.
Type: Buffer Overrun
Risk: Low to High

Summary

mIRC provides scripting capabilities to allow extension of the client. A flaw exists in the \$asctime identifier, which is used to format Unix style time stamps. Passing a string of sufficient length to \$asctime will cause a buffer overflow on the stack. This allows the execution of byte code through calling \$asctime with a carefully constructed string.

The default script included with mIRC does not call \$asctime at any point. However the majority of major scripts available for download call \$asctime to decode data provided by the irc server. Many scripts call \$asctime on data provided from other remote sources. The exploitation of this flaw therefore depends on the script installed by the victim.

NT-Bugtraq: uuuppz.com – Advisory 002 – mIRC \$asctime overflow

-----BEGIN PGP SIGNATURE-----

Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>

iQA/AwUBPWuC4/L9eRNyreu5EQJe3QCgongMQqFL2oZyX1NWicRxdmdXipIAoKb0
YJPJQ+TJoz9kjC2DKkg6m5OJ
=0cKJ

-----END PGP SIGNATURE-----

- *Previous message:* [Kevin Gennuso: "MS02-045 exploit is out"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)