

[UNIX] Netopia Timbuktu Remote Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/22/04

To: list@securiteam.com

Date: 22 Nov 2004 11:28:42 +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>

Netopia Timbuktu Remote Buffer Overflow

SUMMARY

The <<http://www.netopia.com>> Timbuktu software is shipped as "a client/server application that allows remote users to access the desktop of a host system". The server component of this application is vulnerable to a remote buffer overflow vulnerability that, when exploited, causes the server process to crash.

DETAILS

Vulnerable Systems:

* Timbuktu version 7.0.3

Immune Systems:

* Timbuktu version 7.0.4

The server process runs with root privileges on the host Mac OS X and listens for client connections on TCP port 407. By making a number of concurrent connections to this port and repeatedly sending a particular string of data, a memory buffer is overwritten and the server process crashes.

CVE Information:

Securiteam: [UNIX] Netopia Timbuktu Remote Buffer Overflow

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0810>>
CAN-2004-0810

ADDITIONAL INFORMATION

The information has been provided by
<mailto:stephen.de.vries@corsaire.com> Stephen de Vries.

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.