

[NEWS] Novell ZENworks Asset Management Collection Client Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00005.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Dec 2006 14:10:44 +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>

Novell ZENworks Asset Management Collection Client Heap Overflow

SUMMARY

Novell Inc's <<http://www.novell.com/products/zenworks/>> ZENworks is a set of tools used to automate IT management and business processes across the various computing resources within an organization. The Collection Client provides functionality, as a service, that will supply the Collection Server with information regarding the managed machine's hardware and software configuration.

Remote exploitation of an integer overflow vulnerability in Novell Inc.'s ZENworks Asset Management could potentially allow an attacker to execute arbitrary code with SYSTEM privileges on Windows or root on the various supported UNIX based operating systems.

DETAILS

Vulnerable Systems:

* ZENworks Asset Management 7.0 SP1 (7.0.0.36 version of the CClient.exe and Msg.dll files).

A heap overflow may occur when processing specially crafted packets sent

[NEWS] Novell ZENworks Asset Management Collection Client Heap Overflow

to the Collection Client daemon. The root cause of this vulnerability is identical to that of the vulnerability in Msg.dll. For more information please consult the Msg.dll advisory.

Successful exploitation of this vulnerability could allow a remote attacker to take complete control of the affected system.

Vendor Status:

Novell's ZENworks team has addressed this vulnerability within ZENworks 7 Asset Management SP1 IR11. More information can be found by visiting <<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974824.htm>> <http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974824.htm>.

Disclosure Timeline:

- * 10/16/2006 – Initial vendor notification
- * 10/19/2006 – Initial vendor response
- * 12/01/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=447>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=447>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

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.