

[NT] Directory Traversal in Accipiter Direct AdServer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/11/04

To: list@securiteam.com

Date: 11 Jan 2004 12:01:46 +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>

Directory Traversal in Accipiter Direct AdServer

SUMMARY

<<http://www.accipiter.com/>> Accipiter Direct AdServer is "responsible for advertisement handling for badge and banner ads as well as advertisement tracking. The Direct server acts as an http server listening for specially formed requests. It is a proprietary system and cannot be disabled".

A security vulnerability has been found in Accipiter Direct Server 6 that allows retrieval of arbitrary files.

DETAILS

Arbitrary files can be viewed by using the exploit detailed below. Attacker traverses the HTTP server and retrieves arbitrary files by sending specially formed requests through a web browser.

Exploit:

By using the following URL, a remote attacker can access the boot.ini file under the Windows operating system:

<http://accipiterserver/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cboot.ini>

Securiteam: [NT] Directory Traversal in Accipiter Direct AdServer

Workaround:

Vendor will be providing a patch with the next major release. Until then you may run your Accipiter Direct AdServer as an unprivileged user restricted to the webroot.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mbassett@omaha.com> Bassett, Mark.

=====

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.