

# [NEWS] Possible Illegal File Access in Acuma's Acusend

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0130.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 10/25/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 25 Oct 2002 18:18:21 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Possible Illegal File Access in Acuma's Acusend

---

## SUMMARY

Acusend is a leading report portal product from [<http://www.acuma.co.uk>](http://www.acuma.co.uk) Acuma. Acusend allows organizations to collect and collate information from a diverse range of sources and present it via a uniform web interface. Acusend is widely deployed in Government, Education and Aerospace industries. A security vulnerability in the product allows users to access reports they would otherwise not have access to (due to security restrictions).

## DETAILS

Vulnerable systems:

- \* Acusend version 4

During a penetration test of a client's network, Sec-Tec has discovered that it is possible for an authenticated user to access reports belonging to other users if the full URL to the report is known. Although the full URLs may appear to be random, certain factors such as time and date are sometimes used as part of the URL structure, thereby greatly reducing entropy. Release of this information has been withheld awaiting a corrected version from Acuma.

Securiteam: [NEWS] Possible Illegal File Access in Acuma's Acusend

Recommended Action:

The vendor states that the issue is rectified in the latest version.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[davew@sec-tec.com](mailto:davew@sec-tec.com)> David Wray of Sec-Tec.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] IPSwitch WS FTP Server PASV Session Hijacking and PASV Port Scan"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)