

# [NT] Directory Traversal and Log Hogging in Daniel Arenz' Mini Server

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0053.html>

---

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

*Date:* 10/15/02

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

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

Date: 15 Oct 2002 03:44:27 +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.

-----

Directory Traversal and Log Hogging in Daniel Arenz' Mini Server

---

## SUMMARY

Mini Server by Daniel Arenz is a small Windows based web server, two vulnerabilities in the product have been found. One allows attackers to access files residing outside the normally bounding HTML root directory, the second allows attackers to cause the product to no longer log incoming requests (hostile and normal).

## DETAILS

Vulnerable systems:

- \* Mini Server 2.1.6

Immune systems:

- \* Mini Server 3.0.0

There is a directory traversal flaw in Daniel Arenz' Mini Server 2.1.6. It's possible to show every by the web server readable file on the target system by using one of the following URLs:

<http://192.168.0.2/../../../../windows/win.ini>

<http://192.168.0.2/../../../../windows/win.ini>

[http://192.168.0.2/AAA\[...\]/../../../../windows/win.ini](http://192.168.0.2/AAA[...]/../../../../windows/win.ini)

## Securiteam: [NT] Directory Traversal and Log Hogging in Daniel Arenz' Mini Server

It should not be possible to hop through the file system by using some meta-characters (e.g. "..").

Another problem is that the log window has an upper limit for entries. If the window is full, there could no more entries be added. It would make sense to overwrite the first records or clear the whole window after the overflow.

Vendor status:

Marc's email to Daniel was sent on 02/10/12. He acknowledged a day later the vulnerability and wrote, that he'll fix the bug(s) in the upcoming version 3.0.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[marc.ruef@computec.ch](mailto:marc.ruef@computec.ch)> Marc Ruef.

=====

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): "[NEWS] Symantec Enterprise Firewall Secure Webserver Information Leak"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)