

[UNIX] Stronghold Secure Webserver Sample Script Path Disclosure Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0085.html>

From: support@securiteam.com

Date: 05/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 21 May 2002 08:44:39 +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.

Stronghold Secure Webserver Sample Script Path Disclosure Vulnerability

SUMMARY

Red Hat's <http://www.c2.net/> Stronghold is the most mature Apache-based web server available today with over seven years of development and more than 14,000 servers running it to protect their data. Stronghold provides the tools to quickly install and configure the popular Apache Web Server with the security features that customers and business partners expect when they interact with your site. Any user can send a request Stronghold sample script 'swish' causing it to reveal the full path to the web root. In some cases, swish will display system specific information html source code.

DETAILS

Vulnerable systems:

* Stronghold version 3.0

Example:

Accessing the following URL:

<http://host/cgi-bin/search>

Securiteam: [UNIX] Stronghold Secure Webserver Sample Script Path Disclosure Vulnerability

Will reveal in its source code:

```
=====SNIP=====
<HTML>
<HEAD>
<TITLE>Welcome to Stronghold!</TITLE>
</HEAD>

<BODY BGCOLOR="#FFFFFF" TEXT="#000000" VLINK="#FF0000" LINK="#0000FF">

<H1 ALIGN=CENTER>Search Stronghold Documentation</H1>
<hr><form method="POST" action="/cgi-bin/search">
This is a searchable index of information.<br>
<b>Note:</b> <i>This service can only be used from a forms-capable
browser.</i><p>
Enter keyword(s): <input type="text" name="keywords" value="" size=30>
<input type="submit" value=" Search ">
<input type="reset" value=" Reset ">
<p>
<input type="hidden" name="message" value="If you can see this, then your
browser can't support hidden fields.">
<input type="hidden" name="source" value="manual.swish"> (!) <input
type="hidden" name="sourcedir" value="/home/ts/stronghold/swish/"> (!)
<input type="hidden" name="maxhits" value="40">
<input type="hidden" name="sorttype" value="score">
<input type="hidden" name="host" value="">
<input type="hidden" name="port" value="">
<input type="hidden" name="searchprog" value="swish">
<input type="hidden" name="iconurl" value="/icons">
<input type="hidden" name="useicons" value="yes">
</form><hr>
=====SNIP=====
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:ts@securityoffice.net> Tamer Sahin.

```
=====
```

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.

- *Previous message:* support@securiteam.com: "[UNIX] Sun AnswerBook2 Gettransbitmap Buffer Overflow Vulnerability"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)