

Securiteam: [NT] Sambar Webserver DoS Vulnerability (cgitest.exe)

[NT] Sambar Webserver DoS Vulnerability (cgitest.exe)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0112.html>

From: support@securiteam.com

Date: 01/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 23 Jan 2002 23:40:51 +0100 (CET)

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.

Sambar Webserver DoS Vulnerability (cgitest.exe)

SUMMARY

<<http://www.sambar.com/>> Sambar Server is a multi-threaded HTTP server for Microsoft Windows and UNIX systems. A security vulnerability in the web server's default CGIs allows remote attackers to cause the server to crash possibly executing arbitrary code.

DETAILS

Vulnerable systems:

Sambar Webserver version 5.1

Sambar Webserver is bundled with a sample cgi script (testcgi.exe) which create security flaw. Server crashes after sending very long request a few times.

Exploit:

GET /cgi-win/cgitest.exe?AAAAA...(Ax4000)...AAAAA HTTP/1.1

ADDITIONAL INFORMATION

Securiteam: [NT] Sambar Webserver DoS Vulnerability (cgitest.exe)

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: "[NT] Bounce Vulnerability in SpoonFTP"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)