

[NT] SonicWALL Global VPN Client Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Dec 2007 18:06:48 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

SonicWALL Global VPN Client Format String Vulnerability

SUMMARY

The SonicWALL Global VPN Client "provides mobile users with access to mission-critical network resources by establishing secure connections to their office network's IPSec-compliant SonicWALL VPN gateway". SonicWALL Global VPN Client suffers from a format string vulnerability that can be triggered by supplying a specially crafted configuration file. This vulnerability allows an attacker to execute arbitrary code in the context of the vulnerable client. For a successful attack, the attacker would have to entice his victim into importing the special configuration file.

DETAILS

Vulnerable Systems:

- * SonicWall VPN client versions prior to 4.0.0.830

Immune Systems:

- * SonicWall VPN client version 4.0.0.830

Format string errors occur when the client parses the "name" attribute of the "Connection" tag and the content of the "Hostname" Tags in the

ADDITIONAL INFORMATION

The information has been provided by <<mailto:research@xxxxxxxxxxxxxxxx>>
Bernhard Mueller.

The original article can be found at:

<<http://www.sec-consult.com/305.html>> <http://www.sec-consult.com/305.html>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.