

[NEWS] Fortigate Firewall Inadequate Log Filtering

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0041.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/09/03

To: list@securiteam.com

Date: 9 Oct 2003 16:37:14 +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>

Fortigate Firewall Inadequate Log Filtering

SUMMARY

<<http://www.fortinetfirewall.com/>> Fortigate Firewall, has been found to contain a cross-site scripting vulnerability due to inadequate filtering of the log files that is kept when the web filtering is enabled.

DETAILS

Vulnerable systems:

- * Fortigate Firewall pre 2.50 maintenance release 4

Immune systems:

- * Fortigate Firewall 2.50 maintenance release 4

After the web filter has been enabled, the administrator has the ability to review the web filter logs via the web interface. The web filter logs contain the URL that has been denied by the filter. Because of the fact that unwanted characters are not stripped from the denied URL, a remote attacker is able to gain the credentials of an administrator, as soon as the administrator reviews the logs.

Example:

Pages with the keyword "mp3-download" are denied by the web filter. The

Securiteam: [NEWS] Fortigate Firewall Inadequate Log Filtering

page <<http://192.168.5.11/maarten.html>> contains such a keyword. A remote attacker could poison the log files by retrieving "<http://192.168.5.11/maarten.html>< script>alert(oops)</script>

When altering the script a bit, the user credentials could easily be forwarded to the attacker, who could then use these credentials to alter the firewall if the administrator has not properly secured access to HTTPS/SSH/TELNET/HTTP.

Solution:

1. A basic rule in firewall administration is to only allow connections to the firewall—administration—options from specific IP addresses (or preferably, specific IP addresses connecting from a management network to the management interface of the firewall). When this best practice is applied, an attacker that manages to gain administration credentials as described above will not be able to abuse them too easily.
2. Manage your firewall from a dedicated workstation that has no connections (directly OR through a proxy) to un-trusted networks in order to avoid a credential push as described above.
3. Upgrade FortiOS 2.50MR4, which (according to fortinet) does not contain this problem.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:maartenh@phreaker.net>> Maarten Hartsuijker.

=====

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.