

# [NEWS] Fortigate Firewall Web Interface Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0005.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 12/01/03

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

Date: 1 Dec 2003 13:45:46 +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 Web Interface Vulnerabilities

---

## SUMMARY

Several vulnerabilities in web interface of <http://www.fortinetfirewall.com/> Fortigate firewall of which the most serious one will under specific circumstances allow a remote attacker to obtain an administrative username and password of the Fortigate firewall.

## DETAILS

Vulnerable systems:

- \* Fortigate Firewall version pre 2.50 maintenance release 4

Immune systems:

- \* Fortigate Firewall version 2.50 maintenance release 4 (Issue 3)
- \* Fortigate Firewall version 2.50 maintenance release 5 (Issue 1 and 2)

### Issue 1: Improper Input Validation

The variables from several URL's are parsed in the HTML code of the resulting web page. The variables themselves are not sanitized before they are used. Therefore, they can be used to inject code into the admin interface.

## Securiteam: [NEWS] Fortigate Firewall Web Interface Vulnerabilities

The examples below show you a simple alert box, but this could just as well be used to:

- Steal the cookie of the user that is logged in
- Include (for instance) the Cisco homepage into the website that is displayed after clicking the URL

Examples:

<https://IP/firewall/policy/dlg?q=-1&fzone=t><script>alert('oops')</script>>&tzone=dmz

<https://IP/firewall/policy/policy?fzone=internal&tzone=dmz1><script>alert('oops')</script>

<https://IP/antispam/listdel?file=blacklist&name=b><script>alert('oops')</script>&startline=0

<https://IP/antispam/listdel?file=whitelist&name=a><script>alert('oops')</script>&startline=0(natural)

<http://IP/theme1/selector?button=status.monitor.session>"><script>alert('oops')</script>&button\_url=/system/status/status,/system/status/monitor,/system/status/session

[http://IP/theme1/selector?button=status.monitor.session&button\\_url=/system/status/status](http://IP/theme1/selector?button=status.monitor.session&button_url=/system/status/status)"><script>alert('oops')</script>,/system/status/monitor,/system/status/session

[http://IP/theme1/selector?button=status.monitor.session&button\\_url=/system/status/status,/system/status/monitor](http://IP/theme1/selector?button=status.monitor.session&button_url=/system/status/status,/system/status/monitor)"><script>alert('oops')</script>,/system/status/session

[http://IP/theme1/selector?button=status.monitor.session&button\\_url=/system/status/status,/system/status/monitor,/system/status/session](http://IP/theme1/selector?button=status.monitor.session&button_url=/system/status/status,/system/status/monitor,/system/status/session)"><script>alert('oops')</script>

Issue 2: Username and MD5 HASH of Password Stored in Cookie

The username and MD5 hash of the password are stored in a cookie like the one below. When this is combined with the previous XSS vulnerabilities, a remote attacker can trick an administrator into revealing his credentials.

```
cookie=APSCOOKIE=1063444738
%2615
%26FGT-602803043728
%26maarten
%26vsys0
%26$1$2a05ca7c$U7W6SI.7L5ncc7tfZZ7D
```

The password HASH is recognized as FreeBSD's MD5 (probably the base OS of the firewall).

Issue 3: Web Filter Log Passes Unfiltered Session Details

After the web filter has been enabled, the administrator has the ability

## Securiteam: [NEWS] Fortigate Firewall Web Interface Vulnerabilities

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 username and MD5 hash of the password, as soon as the administrator reviews the logs.

An example:

Pages with the keyword "mp3-download" are denied by the web filter. The 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 untrusted networks in order to avoid a credential push as described above.
3. Upgrade FortiOS 2.50MR5, which (according to fortinet) does not contain these problems.

### 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.