

## [NT] FGatePro Multiple Vulnerabilities (Path Disclosure, CSS, Username Exposure)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0012.html>

---

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

*Date:* 09/04/03

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

Date: 4 Sep 2003 18:32:34 +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>

-----  
FGatePro Multiple Vulnerabilities (Path Disclosure, CSS, Username Exposure)  
-----

### SUMMARY

<<http://www.ftgate.com/>> FTGatePro "contains all the features you would expect from a world-class mail server, including anti-virus integration, sophisticated anti-SPAM options, comprehensive IP security features, NT SAM integration, SMTP/ESMTP, web server, web mail, LDAP, POP3, SmartPop, attachment filters, mail filters, system monitoring, MX delivery, dial-up facilities, scheduling, user mailboxes, list mailboxes, group mailboxes, robot mailboxes, autoresponder mailboxes and list servers. FTGatePro is fully compatible with Windows NT/2000/XP".

The product has been found to contain multiple vulnerabilities allowing a remote attacker to cause the server to reveal the true path under which it is installed, to return arbitrary HTML and JavaScript code as if it were its own, and to inform the attacker whether the username he provided is valid or not.

### DETAILS

Vulnerable systems:

Securiteam: [NT] FGatePro Multiple Vulnerabilities (Path Disclosure, CSS, Username Exposure)

\* FTGatePro version 1.22 build 1331

Path Disclosure:

By requesting the following URL:

<http://127.0.0.1:8089/utility/wmsecurity.fts>, the following response will be received:

```
Error in C:\Program Files\FTGate\Webs\WebAdmin\utility\wmsecurity.fts
line 13, Undeclared Identifier 'null'
```

This will allow a remote attacker to reveal the true path under which the product was installed.

Cross Site Scripting:

By requesting such a URL as: [http://127.0.0.1:8089/help/index.fts?href=<script>alert\('C.S.S'\)</script>](http://127.0.0.1:8089/help/index.fts?href=<script>alert('C.S.S')</script>) it is possible to insert malicious HTML and/or JavaScript into pages that are returned by the server (this in turn will allow hijacking of accounts, etc).

Remote User Verification:

Because the server responds differently for invalid usernames and valid username, it is possible to determine whether a user provided username is valid.

Example:

```
Telnet 127.0.0.1 110
```

```
+OK POP3 FTGatePro server ready
user InValid
```

```
-ERR InValid doesn't get mail here
```

```
user user1
```

```
+OK user1 gets mail here
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:vulncode@yahoo.com> Ziv Kamir.

=====

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.

Securiteam: [NT] FGatePro Multiple Vulnerabilities (Path Disclosure, CSS, Username Exposure)

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.