

[UNIX] Net::Server's log() Function Syslog Usage Allows for a Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0147.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/25/05

To: list@securiteam.com

Date: 25 Apr 2005 18:36:18 +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>

Net::Server's log() Function Syslog Usage Allows for a Format String Vulnerability

SUMMARY

The undocumented but frequently used "log" function provided by the Net::Server Perl module is not safe against format string vulnerability.

DETAILS

Vulnerable Systems:

* Net::Server version 0.87

The syslog call in function log is implemented like following:

```
### log only to syslog if setup to do syslog
if( $prop->{log_file} eq 'Sys::Syslog' ){
    $level = $level!~/^\d+$/ ? $level : $Net::Server::syslog_map->{$level}
;
    Sys::Syslog::syslog($level,@_); <----!!!!!!
    return;
}
```

Sys::Syslog tells how to use function "syslog":

Securiteam: [UNIX] Net::Server's log() Function Syslog Usage Allows for a Format String Vulnerability

syslog \$priority, \$format, @args

If \$priority permits, logs (\$format, @args) printed as by "printf(3V)", with the addition that %m is replaced with "\$!"

(the latest error message).

Unfortunately, the function "log" of Net::Server put now the first given log argument into "syslog" function as format string, and the others as arguments.

Workaround:

As a workaround, programs using "log" of Net::Server can replace a single "%" by "%%", but only in case of when syslog is used.

Impact of workaround: programs which call "log" of Net::Server with format string in first log argument will break.

ADDITIONAL INFORMATION

The information has been provided by <mailto:pbieringer@aerasec.de> Dr. Peter Bieringer.

=====

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.