

[UNIX] PFinger Format String Vulnerability (Format String)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0052.html>

From: support@securiteam.com

Date: 12/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Dec 2002 19:06:44 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

PFinger Format String Vulnerability (Format String)

SUMMARY

<<http://www.xelia.ch/unix/pfinger/>> PFinger is an open-source replacement of the GNU Finger daemon. PFinger suffers from a format string vulnerability that, when exploited, can allow the remote execution of arbitrary code.

DETAILS

Vulnerable systems:

- * PFinger version 0.7.8 and earlier

The format string vulnerability arises due to an unsafe call to syslog() in the log() function of log.c

```
.  
syslog(level, syslog_mem);  
.
```

To make this safe a format string should be specified:

Securiteam: [UNIX] PFinger Format String Vulnerability (Format String)

```
.  
syslog(level,"%s", syslog_mem);  
.
```

Due to the way requests are logged the only way to exploit this vulnerability is through setting the DNS name of the fingering host to the attacker supplied format string.

```
h_ent = gethostbyaddr((char *)&remaddr.sin_addr, sizeof(remaddr.sin_addr),  
AF_INET);
```

```
if (h_ent)  
    conn.hostname = strdup(h_ent->h_name);  
else  
    conn.hostname = "(remote)";  
log(LOG_INFO, "Connection from %s  
(%s)",conn.hostname,inet_ntoa(remaddr.sin_addr));
```

This code looks up the Domain name of the fingering host and logs the connection information. This appears to be the only place where user controlled data is logged. For exploitation to succeed the attacker must either control their own DNS, the DNS server of the target host or alternatively spoof the DNS reply. This makes exploitation more difficult but by no means impossible.

Fix Information:

NGSSoftware alerted the author of PFinger with this problem on the 27th of November, 2002. The author has responded and assured NGS that a fix will be implemented shortly. Those who are comfortable with C and cc/gcc can fix these themselves by editing log.c in the manner described in the "Details" section above.

ADDITIONAL INFORMATION

The original advisory can be found at:

<<http://www.nextgenss.com/advisories/pfinger.txt>>
<http://www.nextgenss.com/advisories/pfinger.txt>

The information has been provided by <mailto:nisr@nextgenss.com>
NGSSoftware Insight Security Research.

=====

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: [UNIX] PFinger Format String Vulnerability (Format String)

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.