

[UNIX] Remote Memory Reading Through TCP/ICMP

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0110.html>

From: support@securiteam.com

Date: 01/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 23 Jan 2002 21:07:14 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Remote Memory Reading Through TCP/ICMP

SUMMARY

A security vulnerability in Linux allows remote attackers to cause the remote OS to return chunks of "userland" memory (unrestricted memory). This would pose an information leak, possibly allowing gaining of sensitive information.

DETAILS

Systems affected:

Linux

Solaris

It is possible to read parts of a remote machines memory. To be specific, it would have to be memory recently freed/swapped to disk. Consider this for example:

```
int main(int argc, char **argv[], char **envp[])
{
    char *ptr=0; /* We take a rather large chunk of memory and fill it with
A's */
    int val, i;
```


Securiteam: [UNIX] Remote Memory Reading Through TCP/ICMP

```
+++ linux-work/net/ipv4/icmp.c Sun Jan 20 23:31:29 2002
@@ -495,7 +495,7 @@
 icmp_param.data.icmph.checksum=0;
 icmp_param.csum=0;
 icmp_param.skbn=skbn;
- icmp_param.offset=skbn->nh.raw - skbn->data;
+ icmp_param.offset=skbn->data - skbn->nh.raw;
 icmp_out_count(icmp_param.data.icmph.type);
 icmp_socket->sk->protinfo.af_inet.tos = tos;
 ipc.addr = iph->saddr;
--- linux-work/net/ipv6/icmp.c-o Thu Sep 20 23:12:56 2001
+++ linux-work/net/ipv6/icmp.c Sun Jan 20 23:40:03 2002
@@ -361,7 +361,7 @@
 msg.icmph.icmp6_pointer = htonl(info);

 msg.skbn = skbn;
- msg.offset = skbn->nh.raw - skbn->data;
+ msg.offset = skbn->data - skbn->nh.raw;
 msg.csum = 0;
 msg.daddr = &hdr->saddr;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrewg@tasmail.com> Andrew Griffiths.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Several Windows File Wiping Utilities Do Not Properly Wipe Data under NTFS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)