

Snort ICMP Denial of Service Vulnerability

分類 Denial of Service
 関連ツール名称
 再現性 リモート

技術解説

1) 概要

Free の NIDS (network intrusion detection system:ネットワーク侵入検知システム)であるSnortは、ネットワーク上を流れる悪意あるICMPパケットを検知した際に、パケットの処理が正常に行えず、DoS攻撃が成立してしまう問題がある。

2) 原因

SnortはICMPのデータ部分の最小サイズを8Byteと定義している。この定義により、8Byte未満のICMPパケットを受信した際に、例外処理を行えず、Daemonがクラッシュしてしまう。

Snort ICMP Denial of Service Vulnerability

検証有無

結果 ○: 成功、×: 失敗、-: 未検証

OS	アプリケーション	バージョン	結果
Windows NT SP6a (J)	Snort	1.8.3	○
RedHat 7.1 (J)	Snort	1.8.3	○

検証結果

1) 検証環境

	OS	アプリケーション	備考
攻撃側	RedHat Linux 7.1 J		IP: 192.168.1.211
ターゲット	RedHat Linux 7.1 J	Snort 1.8.3	IP: 192.168.1.208

2) 検証結果

SnortがCoreを出力して、異常終了したのを確認できた。以下はその際の詳細情報である。

```

[root@dhcp08 /]# cd /var/log/snort
[root@dhcp08 snort]# snort -dev host 192.168.1.208 and 192.168.1.211
Log directory = /var/log/snort

Initializing Network Interface eth0

--== Initializing Snort ==--
Checking PID path...
PATH_VARRUN is set to /var/run/ on this operating system
PID stat checked out ok, PID set to /var/run/
Writing PID file to "/var/run/"
Decoding Ethernet on interface eth0

--== Initialization Complete ==--

-*> Snort! <*-
Version 1.8.3 (Build 88)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
01/07-22:59:42.448360 ARP who-has 192.168.1.208 tell 192.168.1.211

01/07-22:59:42.448360 ARP reply 192.168.1.208 is-at 0:50:56:AE:1:3

01/07-22:59:42.448360 ARP reply 192.168.1.208 is-at 0:50:56:AE:1:3

01/07-22:59:42.448360 0:50:56:A2:1:CB -> 0:50:56:AE:1:3 type:0x800 len:0x3C
192.168.1.211 -> 192.168.1.208 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:29 DF
Type:8 Code:0 ID:1229 Seq:0 ECHO
Segmentation fault (core dumped)
[root@dhcp08 snort]#
[root@dhcp08 snort]# ls
192.168.1.208 192.168.1.211 192.168.1.3 core

```

痕跡

1) ログ

*.debugの設定で記録していたsyslogには、この攻撃を特定する内容は存在しなかった。

2) 痕跡

異常終了する直前に、ICMPパケットが流れていることが確認できる。(上記参照) また、snortを起動した際のディレクトリにて、coreが作成される。作成されたcore情報は以下の通りである。

```

[root@dhcp08 snort]# gdb --core=./core
GNU gdb 5.0rh-5 Red Hat Linux 7.1
Copyright 2001 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux".
Core was generated by `snort -dev host 192.168.1.208 and 192.168.1.211'.
Program terminated with signal 11, Segmentation fault.
#0 0x0804e200 in ?? ()
(gdb) q
[root@dhcp08 snort]#

```

影響

SnortにはICMPのサイズ定義について問題がある。そのため、ネットワーク上を流れる悪意あるICMPパケットを検知した際にDoS攻撃が成立してしまう。DoS攻撃が成立した際にはSnortは異常終了する。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2002/1/11現在)

OS	アプリケーション	バージョン	影響	備考
Windows 全般 Unix 全般	Snort	1.8.3 以前	○	

OS、サービス Windows 全般
Unix 全般

アプリケーション Snort 1.8.3 以前

対策方法

1)対策

この問題が対策済みである、パッチを適用する。または、他のNIDSを利用する。

パッチ入手先 URL:

<http://www.securityfocus.com/data/vulnerabilities/patches/snort-icmp.patch>

2)Advisory情報