Falha de autenticação SSH devido a condições de memória baixas

Contents

Introduction

Este documento descreve o problema em um roteador Cisco IOS® quando o Secure Shell (SSH) para o roteador às vezes falha com uma falha de autenticação de usuário relatada nas depurações SSH. Esse problema ocorre mesmo que as credenciais de usuário inseridas estejam corretas e as mesmas credenciais funcionem corretamente para Telnet.

> **Note**: O bug da Cisco ID CSCum19502 foi arquivado para tornar o comportamento entre SSH e Telnet consistente.

Problema

Observe nessas depurações que, mesmo que "debug aaa authentication" esteja ativado, não há depurações de Autenticação, Autorização e Contabilidade (AAA) sendo impressas para mostrar que AAA é chamada e retorna a falha.

```
Router#show debug
General OS:
AAA Authentication debugging is on
SSH:
Incoming SSH debugging is on
ssh detail messages debugging is on
Router#
*Sep 30 20:28:57.172: SSH2 2: MAC compared for #8 :ok
*Sep 30 20:28:57.172: SSH2 2: input: padlength 15 bytes
*Sep 30 20:28:57.172: SSH2 2: Using method =
keyboard-interactive
*Sep 30 20:28:57.172: SSH2: password authentication failed
for cisco
*Sep 30 20:28:59.172: SSH2 2: send:packet of length 64
(length also includes padlen of 14)
*Sep 30 20:28:59.172: SSH2 2: computed MAC for sequence
no.#8 type 51
*Sep 30 20:29:01.751: SSH2 2: ssh_receive: 144 bytes received
*Sep 30 20:29:01.751: SSH2 2: input: total packet length of
128 bytes
*Sep 30 20:29:01.751: SSH2 2: partial packet length(block size)
16 bytes,needed 112 bytes,
```

Às vezes, o syslog mostrado aqui também é observado quando o SSH é tentado, mas não é impresso consistentemente:

```
*Sep 30 20:23:27.598: %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming
calls due to insufficient processor memory
```

A causa raiz do problema são as condições de memória baixa no roteador. Quando o AAA não aloca a memória para criar o UID exclusivo para a sessão SSH recebida, ele relata a mesma falha de uma falha de autenticação AAA mesmo que o AAA não seja tentado. Essa condição ocorre quando a memória livre do processador cai abaixo do "limiar de memória baixa de autenticação" AAA, que por padrão é definido como 3% da memória total e pode ser verificado com o comando **show aaa memory**. Esse problema é frequentemente visto em uma plataforma ASR (Aggregation Services Router) 1001, na qual há memória limitada no roteador que pode ser esgotada com o uso pesado do plano de controle, como uma tabela BGP (Border Gateway Protocol) completa. No ASR 1001 há 4 GB de DRAM instalada, mas depois que todos os outros processadores de CPUs e Linux inicializam, o Cisco IOS obtém os 1,1 GB restantes. Quando a memória é esgotada a ponto de o AAA não poder mais alocar memória para o UID, o SSH falha ao funcionar.

Considere estes dados de memória de dois ASRs:

```
SSH Not Working:
----------------
ASR1#show memory summary
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7FE150387010 1160982064 1146067400 14914664 14225352 13918620
lsmpi_io 7FE14FB7E1A8 6295128 6294304 824 824 412

SSH Working:
------------
ASR2#show memory summary
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7FFB6ACB0010 1160982064 1120122056 40860008 29163912 24132068
lsmpi_io 7FFB6A4A71A8 6295128 6294304 824 824 412
```

A partir de um cálculo simples, no ASR inoperante, a porcentagem de memória livre é de 1,28% (14914664 / 1160982064 * 100) do total de memória disponível. No ASR funcional, é de 3,51% (40860008 / 1160982064 * 100), que está logo acima do limite de memória baixa de autenticação.

Esse problema é difícil de identificar porque a mensagem %AAA-3-ACCT_LOW_MEM_UID_FAIL frequentemente não é impressa quando esse erro ocorre devido à condição de memória baixa. Além disso, a forma como a AAA calcula o limite de memória não depende da quantidade bruta de memória do processador disponível no RP (Route Processor, processador de rota), mas sim de uma porcentagem da memória total. Portanto, ainda pode haver muita memória do processador mostrada como livre na saída do **comando show memory summary** quando isso ocorre sem falhas de malloc reportadas.

> **Note**: O bug da Cisco ID CSCuj50368 foi arquivado para tornar as mensagens de erro SSH mais explícitas sobre o motivo real da falha de autenticação.

Uma forma de verificar se esse é realmente o problema é examinar as estatísticas de memória AAA:

```
Router#show aaa memory
Allocator-Name In-use/Allocated Count
------------------------------------------------------------------------
AAA AttrL Hdr : 0/65888 ( 0%) [ 0] Chunk
```

```
AAA AttrL Sub : 0/65888 ( 0%) [ 0] Chunk
AAA DB Elt Chun : 544/65888 ( 0%) [ 4] Chunk
AAA Unique Id Hash Table : 8196/8288 ( 98%) [ 1]
AAA chunk : 0/16936 ( 0%) [ 0] Chunk
AAA chunk : 0/16936 ( 0%) [ 0] Chunk
AAA Interface Struct : 1600/1968 ( 81%) [ 4]

Total allocated: 0.230 Mb, 236 Kb, 241792 bytes


AAA Low Memory Statistics:
_____________________________
Authentication low-memory threshold : 3%
 Accounting low-memory threshold : 2%


 AAA Unique ID Failure : 96
Local server Packet dropped : 0
CoA Packet dropped : 0
PoD Packet dropped :
```

Se a contagem de "Falha de ID Exclusiva de AAA" incrementar em cada tentativa de SSH com falha, o problema é causado por essa condição de memória baixa.

Para solucionar esse problema, as etapas padrão de solução de problemas de memória ASR 1000 devem ser seguidas para isolar a causa. Para obter mais informações sobre como solucionar problemas de memória no ASR, consulte Visão geral de uso da memória.

Solução

Para solucionar esse problema, devem ser tomadas as etapas padrão de solução de problemas de memória do roteador. As etapas isolam se o problema é devido ao uso normal, caso em que uma atualização de plataforma/memória pode ser justificada; ou um vazamento de memória no qual pode ser necessário monitorar e solucionar problemas adicionais de memória. Consulte Detector de vazamento de memória e técnicas comuns de solução de problemas de memória para obter mais detalhes.

Para versões que não têm a correção do bug da Cisco ID CSCum19502 , a solução mais óbvia é habilitar o Telnet ou o acesso do console ao roteador, já que somente o SSH é afetado por esse limite.

> **Tip**: O comando **aaa memory threshold** permite reduzir os valores de limite para um mínimo de 1%. No entanto, embora isso forneça uma maneira temporária de SSH para o roteador, pode levar a outras implicações, como a permissão de utilização da memória do processador para cair muito pouco antes dos administradores serem alertados. Isso pode fazer com que processos mais importantes, como o BGP que usa grandes quantidades de memória, não funcionem mais. Por isso, é algo que deve ser usado com cautela.

Como explicado anteriormente, é completamente plausível que o roteador não vaze memória, mas apenas tenha uma assinatura excessiva para os recursos habilitados. Nesse caso, uma atualização de plataforma/memória pode ser garantida.