Autenticação SSH falha devido às condições de memória baixa

Índice

Introdução

Este documento descreve a edição em um roteador do ® do Cisco IOS quando o Shell Seguro (ssh) ao roteador falha às vezes com uma falha relatada da autenticação de usuário no SSH debuga. Esta edição ocorre mesmo que as credenciais do usuário incorporadas estejam corretas e as mesmas credenciais trabalhem corretamente para o telnet.

> Nota: A identificação de bug Cisco CSCum19502 foi arquivada a fim fazer o comportamento entre o SSH e o telnet consistentes.

Problema

A observação nestes não debuga que mesmo que “debugar a autenticação aaa” está permitida, lá é nenhum Authentication, Authorization, and Accounting (AAA) debuga ser imprimido para mostrar o AAA realmente é invocada 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,
```

O Syslog mostrado aqui é observado às vezes igualmente quando o SSH é tentado, mas não obtém impresso consistentemente:

```
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,
```

A causa de raiz do problema é condições de memória baixa no roteador. Quando o AAA não atribui a memória para criar o ID exclusivo (UID) para a nova sessão SSH, relata a mesma falha que uma falha da autenticação de AAA mesmo que o AAA não seja tentado. Esta circunstância ocorre quando a memória livre do processador cai abaixo do AAA da “ponto inicial da memória baixa autenticação”, que à revelia está ajustado a 3% da memória total e podido ser verificado com o **comando memory aaa da mostra**. Este problema é considerado frequentemente em uma plataforma 1001 do roteador dos serviços da agregação (ASR) onde haja uma memória limitada no roteador que pode ser esgotado com uso pesado do plano do controle, tal como uma tabela completa do Border Gateway Protocol (BGP). No ASR 1001 há 4GB do DRAM instalados, mas após a bota de todos os outros processadores CPU e de Linux Cisco IOS obtém os 1.1 GB deixados sobre. Uma vez que a memória é esgotada ao ponto que o AAA pode já não atribuir a memória para o UID, o SSH não trabalha.

Considere estes dados da memória de dois ASR:

```
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
```

De um cálculo simples, no ASR nonworking a porcentagem da memória livre é 1.28% (14914664/1160982064 * 100) da memória disponível total. No ASR de trabalho é 3.51% (40860008/1160982064 * 100), que está apenas acima do ponto inicial da memória baixa da autenticação.

Este problema é difícil de identificar porque a mensagem %AAA-3-ACCT_LOW_MEM_UID_FAIL frequentemente não obtém impressa quando este erro ocorre devido à condição de memória baixa. Além disso, a maneira que o AAA calcula o ponto inicial da memória não depende da quantidade crua de memória de processador disponível no route processor (RP), mas um pouco

de uma porcentagem da memória total. Consequentemente, pôde ainda haver convenientemente uma abundância da memória de processador mostrada como livre no **comando show memory summary** output quando este ocorre sem as falhas de malloc relatadas.

> Nota: A identificação de bug Cisco CSCuj50368 foi arquivada a fim fazer Mensagens de Erro SSH mais explícitos sobre o motivo real para a falha de autenticação.

Uma maneira a de verificar se este é certamente o problema é olhar as estatísticas da 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 da falha do ID exclusivo AAA” incrementa com cada tentativa falhada SSH, o problema está causado por esta condição de memória baixa.

A fim pesquisar defeitos esta edição, os passos de Troubleshooting da memória do padrão ASR 1000 devem ser ordem recolhida para isolar a causa. Para obter mais informações sobre de como pesquisar defeitos edições da memória no ASR, veja a vista geral da utilização de memória.

Solução

A fim pesquisar defeitos esta edição, os passos de Troubleshooting padrão da memória de roteador devem ser tomados. O isolado das etapas se o problema é devido ao uso normal, neste caso uma plataforma/upgrade de memória pôde ser justificada; ou um escape de memória onde a monitoração adicional e o Troubleshooting da memória puderam ser exigidos. Veja o detector de escape de memória e técnicas de Troubleshooting comuns da memória para mais detalhes.

Para as versões que não têm o reparo da identificação de bug Cisco CSCum19502, a ação alternativa a mais óbvia é permitir o telnet ou o acesso de console ao roteador, desde que somente o SSH é afetado por este ponto inicial.

> Dica: O comando threshold da memória aaa permite que você reduza os valores de limiar a

um mínimo de 1%. Contudo, quando este fornecer uma maneira provisória ao SSH ao roteador, pode conduzir a outras implicações tais como a permissão da utilização da memória de processador para deixar cair realmente baixo antes que os admins estejam alertados. Isto pôde fazer com que uns processos mais importantes, tais como o BGP que se usa acima das grandes quantidades de memória, já não trabalhem. Daqui este é algo que deve ser usado com cuidado.

Como explicado mais cedo, é completamente plausível que o roteador não escapa a memória mas é apenas oversubscribed para as características permitidas. Neste caso uma plataforma/upgrade de memória pôde ser justificada.