Pesquise defeitos problemas de pesquisa de diretório do Jabber de Cisco

Índice

Introdução

Este documento descreve como pesquisar defeitos Cisco Jabber o problema de pesquisa de diretório quando o Secure Socket Layer (SSL) é configurado.

Contribuído por Khushbu Shaikh, engenheiros de TAC da Cisco. Editado por Sumit Patel e por Jasmeet Sandhu

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Jabber para Windows
- Wireshark

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Problema

A pesquisa de diretório do Jabber não trabalha quando o SSL é configurado.

Análise do log do Jabber

Os logs do Jabber mostram este erro:

```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

2016-10-21 08:35:47,004 DEBUG [0x000034ec] [rdsource\ADPersonRecordSourceLog.cpp(50)]
[csf.person.adsource] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - Using
custom credentials to connect [LDAP://gbllidmauthp02.sealedair.corp:389] with tokens [1]


2016-10-21 08:35:47,138 DEBUG [0x000034ec] [rdsource\ADPersonRecordSourceLog.cpp(50)]
[csf.person.adsource] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - failed
to get a searcher - COMException [0x80072027]
```

Análise da captura de pacote de informação

Nesta captura de pacote de informação, pode-se ver que a conexão de Protcol do controle de transmissão (TCP) ao server do diretório ativo (AD) é bem sucedido mas a saudação de SSL entre o cliente e o server do Lightweight Directory Access Protocol (LDAP) falha. Isto faz com que o Jabber envie uma mensagem FIN em vez da chave de sessão de criptografia para a comunicação.

343	2016-10-26 17:16:41.086863000	10.8.64.32	172.22.174.228	TCP	66 54155→636 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
344	2016-10-26 17:16:41.093563000	172.22.174.228	10.8.64.32	TCP	66 636→54155 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_P
345	2016-10-26 17:16:41.093640000	10.8.64.32	172.22.174.228	TCP	54 54155→636 [ACK] Seq=1 Ack=1 Win=65536 Len=0
346	2016-10-26 17:16:41.093988000	10.8.64.32	172.22.174.228	TLSv1	191 Client Hello
347	2016-10-26 17:16:41.100193000	172.22.174.228	10.8.64.32	TCP	60 636→54155 [ACK] Seq=1 Ack=138 Win=15680 Len=0
348	2016-10-26 17:16:41.102128000	172.22.174.228	10.8.64.32	TLSv1	1423 Server Hello
349	2016-10-26 17:16:41.102128000	172.22.174.228	10.8.64.32	TCP	1423 [TCP segment of a reassembled PDU]
350	2016-10-26 17:16:41.102129000	172.22.174.228	10.8.64.32	TLSv1	115 Certificate
351	2016-10-26 17:16:41.102180000	10.8.64.32	172.22.174.228	TCP	54 54155→636 [ACK] Seq=138 Ack=2800 Win=65536 Len=0
352	2016-10-26 17:16:41.102914000	10.8.64.32	172.22.174.228	TCP	54 54155→636 [FIN, ACK] Seq=138 Ack=2800 Win=65536 Len=0
353	2016-10-26 17:16:41.104996000	10.8.64.32	172.22.180.59	TCP	66 54156→636 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
354	2016-10-26 17:16:41.108922000	172.22.174.228	10.8.64.32	TCP	60 636→54155 [FIN, ACK] Seq=2800 Ack=139 Win=15680 Len=0

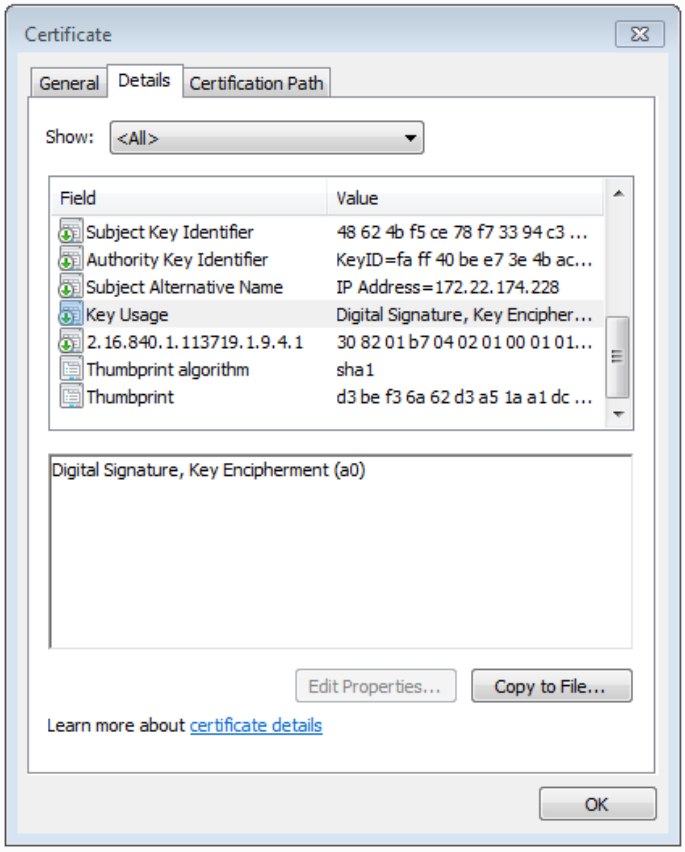
A edição ainda persiste mesmo que o certificado assinado AD seja transferido arquivos pela rede à loja da confiança do cliente o PC.

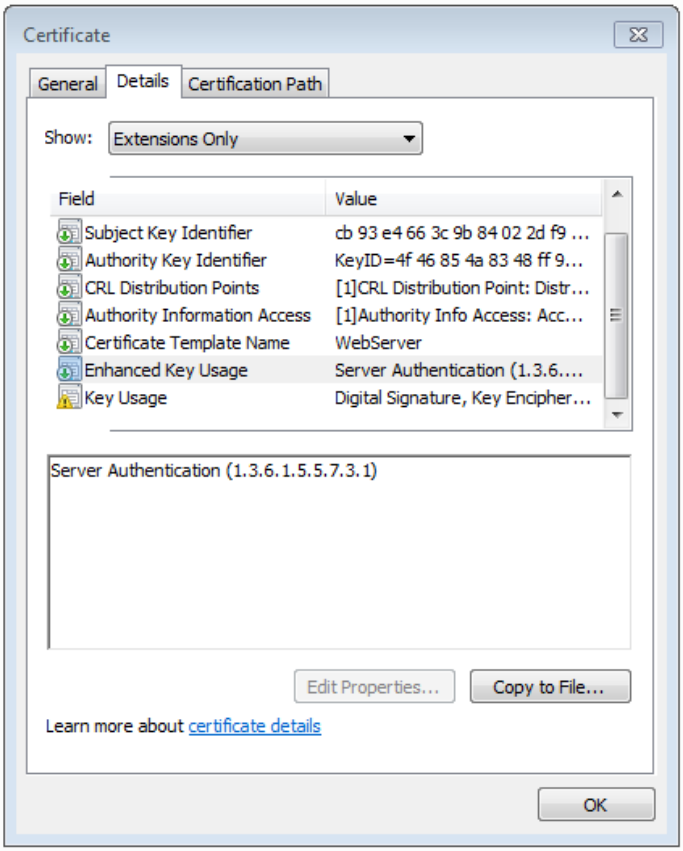
Analisa mais da captura de pacote de informação revela que a autenticação de servidor está ida na seção do Enhanced Key Usage do certificado de servidor AD.

```
Certificate: 308205463082042ea0030201020224021c11ffa5290aa0e3... (id-at-commonName=gbllidmauthp01.sealedair.corp,id-at-organi:
  signedCertificate
    version: v3 (2)
    serialNumber: 0x021c11ffa5290aa0e3110e51ee38b93ad70008edb0ec5c9b...
    signature (sha1WithRSAEncryption)
    issuer: rdnSequence (0)
      rdnSequence: 2 items (id-at-organizationName=SAC_AUTH_PROD,id-at-organizationalUnitName=Organizational CA)
    validity
    subject: rdnSequence (0)
      rdnSequence: 2 items (id-at-commonName=gbllidmauthp01.sealedair.corp,id-at-organizationName=SAC_AUTH_PROD)
    subjectPublicKeyInfo
    extensions: 5 items
      Extension (id-ce-subjectKeyIdentifier)
      Extension (id-ce-authorityKeyIdentifier)
      Extension (id-ce-subjectAltName)
      Extension (id-ce-keyUsage)
        Extension Id: 2.5.29.15 (id-ce-keyUsage)
        Padding: 5
        KeyUsage: a0 (digitalSignature, keyEncipherment)
      Extension (pa-sa)
        Extension Id: 2.16.840.1.113719.1.9.4.1 (pa-sa)
        SecurityAttributes
          versionNumber: 0100
          nSI: True
          securityTM: Novell Security Attribute(tm)
          uriReference: http://developer.novell.com/repository/attributes/certattrs_v10.htm
          gLBExtensions
  algorithmIdentifier (sha1WithRSAEncryption)
  Padding: 0
```

Solução

Uma encenação foi recreada com um certificado que tivesse a autenticação de servidor no Enhanced Key Usage que resolveram a edição. Veja as imagens dos Certificados para a comparação.





O identificador da autenticação de servidor no certificado é uma condição prévia para uma saudação de SSL bem sucedida.

Informações Relacionadas

https://www.petri.com/enable-secure-ldap-windows-server-2008-2012-dc