Hoe kan ik ervoor zorgen dat mijn ESA alleen SSH-verbindingen accepteert van klanten die SSH v2 gebruiken?

Inhoud

Inleiding

Dit document beschrijft hoe u SSH-verificatieversies kunt bekijken en configureren op de Cisco e-mail security applicatie (ESA).

Hoe kan ik ervoor zorgen dat mijn ESA alleen SSH-verbindingen accepteert van klanten die SSH v2 gebruiken?

Het ESA kan worden ingesteld om Secure Shell (SSH)-verbindingen toe te staan. SSH-verbindingen versleutelen het verkeer tussen de verbindingshost en de ESA. Dit beschermt authenticatie informatie zoals gebruikersnaam en wachtwoorden. Er zijn twee belangrijke versies van het SSH-protocol: versie 1 (SSH v1) en versie 2 (SSH v2). SSH v2 is, aangezien het recentelijker is, veiliger dan SSH v1, en daarom geven veel ESA-beheerders er de voorkeur aan alleen verbindingen toe te staan van klanten die SSH v2 gebruiken.

Op versies van AsyncOS door 7.6.3, kan het uitschakelen van SSH v1 verbindingen vanaf de CLI met **sshConfiguration** geschieden:

```
mail3.example.com> sshconfig
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
[]> setup
SSH v1 is currently ENABLED.
Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> DISABLE
```

Op versies van AsyncOS 8.x en nieuwer bestaat de optie om SSH v1 uit te schakelen niet met **sshConfiguration**. Als SSH v1 voor de upgrade van 8.x is ingeschakeld, blijft SSH v1

ingeschakeld en toegankelijk op de ESA, zelfs nadat de upgrade voltooid is, hoewel alle ondersteuning voor SSH v1 is verwijderd. Dit kan een probleem zijn voor beheerders die regelmatige veiligheidscontroles en penetratietests uitvoeren.

Aangezien alle ondersteuning voor SSH v1 is verwijderd, moet een ondersteuningsverzoek worden geopend om SSHv1 uitgeschakeld te krijgen.

Start de volgende opdracht vanaf een externe Linux/Unix-host of een andere toepasselijke CLI-verbinding van keuze, om te bevestigen of SSH v1 aan de betrokken ESA is ingeschakeld of uitgeschakeld:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

De verwachte uitvoer is "Protocol belangrijke versies verschillen: 1 vs. 2", wat zou betekenen dat SSH v1 uitgeschakeld is. Als dit niet het geval is en SSH v1 nog beschikbaar is, ziet u:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Password:
Response:
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
Copyright (c) 2001-2013, Cisco Systems, Inc.

AsyncOS 8.0.1 for Cisco IronPort C360 build 023

Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
myesa.local>
```

Deze uitvoer zou een signaal zijn dat SSH v1 nog steeds in gebruik is en onveiligheid kan veroorzaken met de ESA na aanpassing aan 8.x of nieuwer. Dit kan onder de aandacht worden gebracht door middel van een penetratietest of een veiligheidscontrole en door een significante kloof te identificeren. Om deze correctie te kunnen corrigeren, moet u een ondersteuningscase openen en vragen om deze te laten corrigeren. U moet een ondersteuningstunnel van het ESA kunnen leveren voor Cisco Technical Support.

Gerelateerde informatie

- CSCuo46017: SSHv1 blijft ingeschakeld na de upgrade en kan niet worden uitgeschakeld
- Cisco e-mail security applicatie – eindgebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems