vESA kann keine Updates für Antispam oder Antivirus herunterladen und anwenden.

Inhalt

Einführung

Dieses Dokument beschreibt, wenn eine virtuelle E-Mail-Security-Appliance (vESA) keine Updates für die Cisco Antispam-Engine (CASE) oder Sophos und/oder McAfee-Antivirus herunterlädt und anwendet, obwohl die virtuelle Appliance ordnungsgemäß lizenziert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- E-Mail Security Appliance (ESA)
- vESA, Virtual Web Security Appliance (vWSA), Virtual Security Management Appliance (vSMA)
- AysncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- vESA, das AsyncOS 8.0.0 und höher ausführt
- vWSA, die AsyncOS 7.7.5 und höher ausführt
- vSMA, der AsyncOS 9.0.0 und höher ausführt

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

vESA kann keine Updates für Antispam oder Antivirus herunterladen und anwenden.

Wenn Sie Antispam oder Antivirus aktualisieren, sind die Prozesse nicht in der Lage, die Service-Engine oder die Regeln zu aktualisieren, selbst wenn Sie den Befehl **update force** eingeben.

Einer dieser Befehle wurde möglicherweise direkt über die CLI auf der vESA eingegeben:

```
> antispamupdate ironport
>antispamupdate ironport force
>antivirusupdate force
>updatenow force
```

Wenn Sie **tail updater_logs** ausführen, ähneln die festgestellten Fehler den folgenden:

```
Mon Oct 21 17:48:43 2013 Info: Dynamic manifest fetch failure: Received invalid update manifest
response
```

Dies weist darauf hin, dass der dynamische Host-URL, der der Aktualisierungskonfiguration zugeordnet ist, nicht in der Lage ist, das richtige Aktualisierungsmanifest zu erreichen. Der dynamische Host-URL wird im **Befehl updateconfig** festgelegt. Der Unterbefehl **dynamichost** ist ein ausgeblendeter Befehl innerhalb **von updateconfig**, wie hier hervorgehoben:

```
myesa.local> updateconfig
Service (images): Update URL:
-------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
IMS Secondary Service rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]> dynamichost
```

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]>
```

Stellen Sie die Appliance so ein, dass der richtige dynamische Host-URL verwendet wird.

Es gibt zwei verschiedene dynamische Host-URLs, die für Kunden verwendet werden, je nachdem, wie sie über Cisco verknüpft sind:

1. update-manifests.sco.cisco.com:443 Verwendung: Kunden-vESA, vWSA, vSMA
2. stage-stg-updates.ironport.com:443 Verwendung: Freundliche, virtuelle und Hardware-Appliances der Beta-Serie

   Hinweis: Hardware-Appliances (C1x0, C3x0, C6x0 und X10x0) sollten NUR die dynamische Host-URL von *update-manifests.ironport.com:443* verwenden. Wenn eine Clusterkonfiguration mit ESA und vESA vorhanden ist, muss **updateconfig** auf Computerebene konfiguriert werden und dann entsprechend **dynamichost** festgelegt werden.

   Hinweis: Kunden sollten die Staging Update Server-URLs nur dann verwenden, wenn sie Zugriff auf die Vorabbereitstellung durch Cisco nur für die Beta-Nutzung erhalten haben. Wenn Sie keine gültige Lizenz für die Verwendung von Beta beantragt haben, erhält Ihre Appliance keine Updates von den Staging-Update-Servern.

Geben Sie als Fortsetzung von **updateconfig** und dem Unterbefehl **dynamichost** bei Bedarf den dynamischen Host-URL ein, kehren Sie zur Hauptaufforderung der CLI zurück, und bestätigen Sie die Änderungen:

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]> stage-stg-updates.ironport.com:443
[]> <<<HIT RETURN TO GO BACK TO THE MAIN CLI PROMPT>>>

myesa.local> commit
```

Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob die Appliance jetzt die richtige dynamische Host-URL erreicht und Updates erfolgreich sind:

1. Erhöhen Sie die **updater_logs** auf **debug**.

```
Currently configured logs:> logconfig

Log Name Log Type Retrieval Interval
-------------------------------------------------------------------------------
1. antispam Anti-Spam Logs Manual Download None
[SNIP FOR BREVITY]
28. updater_logs Updater Logs Manual Download None
29. upgrade_logs Upgrade Logs Manual Download None
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
```

```
[]> edit
Enter the number of the log you wish to edit.
[]> 28 [NOTE, log # will be different on a per/appliance basis]
Please enter the name for the log:
[updater_logs]>
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
[SNIP FOR BREVITY]

myesa_2.local> commit
```

2. Führen Sie ein gewaltsames Update entweder für Antispam (**antispamupdate force**) oder für Antivirus (**antivirusupdate force**) aus.
```
myesa.local> antivirusupdate force

Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```
3. Schließlich **tail updater_logs** und stellen Sie sicher, dass die Appliance den Dynamichost wie angegeben erreichen kann:
```
Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-
updates.ironport.com:443
```

Fehlerbehebung

Gehen Sie wie folgt vor, um Probleme zu beheben:

1. Stellen Sie sicher, dass die Standard-**Aktualisierungskonfiguration** verwendet wird. Wenn sich die vESA oder der Host hinter einer Firewall befindet, stellen Sie sicher, dass Updates mit einem statischen Server verwendet werden.
2. Stellen Sie sicher, dass Sie **Telnet** zur ausgewählten dynamischen Host-URL bereitstellen können:
```
> telnet
Please select which interface you want to telnet from.
1. Auto
2. Management (172.16.6.165/24: myesa_2.local)
3. new_data (192.168.1.10/24: myesa.local_data1)
[1]>
Enter the remote hostname or IP address.
[]> stage-stg-updates.ironport.com
Enter the remote port.
[25]> 443
Trying 208.90.58.24...
Connected to stage-stg-updates.ironport.com.
Escape character is '^]'.
^] ["CTRL + ]"]
telnet> quit
Connection closed.
```

Zugehörige Informationen

- Content Security Appliance-Upgrades oder -Updates mit einem statischen Server
- Technischer Support und Dokumentation - Cisco Systems