Fehlerbehebung bei Pufferkonfiguration unter rechtmäßigem Interception Context in StarOS

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für die "Pufferkonfiguration" unter dem Kontext für rechtmäßiges Abfangen in StarOS beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie StarOS kennen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Abkürzungen

LI	Rechtmäßiges Abfangen von Daten
LEA	Strafverfolgungsbehörde
AF	Zugriffsfunktion
MF	Mediationsfunktion
DF	Zustellungsfunktion
CF	Kontrollfunktion
IRI	Zugehörige Informationen abfangen

CC	Inhalt der Kommunikation
CLI	Befehlszeilenschnittstelle

AF kann ein beliebiger StarOS-Knoten sein. CF hat seinen Sitz in den Geschäftsräumen oder der Verwaltungsdomäne von LEA.

Problem

Zum Zeitpunkt der Konfiguration der Pufferungsoption unter dem Lawful Interception-Modul wurde festgestellt, dass der Parameter für die ereignis-/inhaltsbasierte Pufferungsoption in der CLI-Konfigurationsliste nicht verfügbar war.

Mit dieser Option können Sie den Pufferwert von 5.000 IRI-Standarddatensätzen und 1.000 CC-Datensätzen pro LI-Kontext definieren.

Die einzige in der Konfigurationsliste verfügbare Option war "dest-addr".

```
[li-context]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
```

Im Idealfall sollte das Schlüsselwort "buffer" zusammen mit der Option "dest-addr" in der zuvor erwähnten Liste von Optionen angezeigt werden.

Rechtmäßiges Abfangen von Daten

> **Anmerkung:** Lawful Intercept ist eine lizenzaktivierte Funktion. Die Basic Lawful Intercept-Lizenz unterstützt UDP als Transportprotokoll für das Abfangen von Anrufinhalten für aktive Teilnehmer. Event-Interception (IRI) und TCP als Transportprotokoll für die Übermittlung werden unter der Basic-Lizenz nicht unterstützt. Die Enhanced Lawful Intercept-Lizenz unterstützt alle Funktionen der Basic LI-Lizenz sowie Event (IRI) Interception und TCP als Transportprotokoll für die Übermittlung abgefangener Pakete.

Die Lawful Intercept-Funktion bietet dem Netzbetreiber die Möglichkeit, Steuerungs- und Datennachrichten der angegriffenen mobilen Benutzer abzufangen. Um diese Unterstützung in Anspruch zu nehmen, fordert die LEA den Netzbetreiber auf, mit der Überwachung eines bestimmten Mobilfunknutzers zu beginnen. Dieser Antrag wird durch einen Gerichtsbeschluss oder einen Haftbefehl unterstützt. In verschiedenen Ländern werden unterschiedliche Standards für das Abfangen von Gesetzen befolgt.

Ein typischer Prozess zum rechtmäßigen Abfangen umfasst folgende Ereignisabfolge:

1. Die LEA fordert den TSP auf, mit dem Abfangen einer Sitzung einer bestimmten Person zu beginnen, die in der Regel durch einen Gerichtsbeschluss oder einen Haftbefehl unterstützt werden muss. Es werden Informationen zur Identifizierung der Person bereitgestellt (z. B.

Telefonnummer oder Name/Adresse usw.).
2. Der TSP-Administrator konfiguriert die TSP-Zugriffsfunktion/-Bereitstellungsfunktion, um das Abfangen von Steuerungs-/Datenereignissen des Zielteilnehmers zu starten. Wenn die Teilnehmersitzung bereits läuft, wird die Überwachung sofort durchgeführt. Andernfalls muss die Zugriffsfunktion warten, bis die Teilnehmersitzung eine Verbindung herstellt.
3. Die Zugriffsfunktion sendet eine Kopie der Steuerungs-/Datenereignisse für die abgefangene Sitzung an die Zustellungsfunktion.
4. Die Zustellungsfunktion sendet die abgefangenen Informationen an eine oder mehrere Erfassungsfunktionen, die sich im Verwaltungsbereich der LEA befinden. Eine Collection-Funktion analysiert und speichert die abgefangenen Informationen.
5. Wenn die LEA das Beenden des Interception anfordert, konfiguriert der TSP-Administrator die Zugriffsfunktion und die Zustellungsfunktion, um das Interception für diese bestimmte Teilnehmersitzung zu beenden.

Eine CLI (Command Line Interface) über SSH-Sitzung wird vom DF für die LI-Bereitstellung und -Aufhebung der Bereitstellung der Zielidentität sowie zur Überwachung der LI-Statistiken verwendet.

Diese Protokolle/Modi (IPv4 und IPv6) werden von StarOS unterstützt, um LI-Ereignisse und -Inhalte an DF zu übermitteln:

- UDP-Modus (Un-ack): Die Adressen von DF2 und DF3 werden zum Zeitpunkt der Bereitstellung für den UDP-Unbestätigtmodus bereitgestellt.
- TCP-Modus: Für den TCP-Modus wird in der Konfiguration nur die Peer-Adresse angegeben. Die gesamte Übermittlung abgefangener Ereignisse (IRI) wird an DF2 und die Übermittlung aller abgefangenen Daten (CC) an DF3 gesendet.

Fehlerbehebung

Die StarOS-Konfiguration sollte über eine entsprechende Lizenz für diese Funktion verfügen.

```
[local]<hostname># show license information | grep -i lawful
Monday December 10 01:54:13 UTC 2018
Lawful Intercept [ ASR5K-XX-CSXZZLI ]
+ Enhanced Lawful Intercept [ ASR5K-XX-CS0ZZELI / ASR5K-00-CS00XZI ]
Persistent Lawful Intercept [ ASR5K-XX-CS1ZZPLI ]
Segregating Lawful Intercept Context based on Count [ ASR5K-XX-PWXZZICS ]
```

StarOS sollte außerdem über eine "separate li-Konfiguration" verfügen.

Mit dieser Funktion kann nur "li-administrator" die Integrationsdetails der LI-Schnittstelle in einem dedizierten li-Kontext anzeigen und bearbeiten.

Der LI-Admin-Benutzer sollte in der Konfiguration li-administration zugeordnet werden.

```
administrator liadmin encrypted password *** ftp li-administration
```

Es wurde jedoch festgestellt, dass StarOS die Definition der Pufferoption im Lawful-Intercept-Konfigurationsmodul nicht erlaubte.

```
[local]<hostname># context li
```

```
[li]<hostname># config
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
====> customer do see only this option

[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery buff
Unknown command - "buff", unrecognized keyword
```

Im Idealfall sollte eine Option mit dem Schlüsselwort "buffer" angezeigt werden, um die CLI so für die Pufferkonfiguration zu vervollständigen.

```
configure
context
lawful-intercept tcp event-delivery buffer max-limit <1000 ... 50000>
end
```

Auflösung

Um die li-admin-Rechte für alle StarOS-Benutzer zu erhalten, sollte dieser Benutzer unter li context mit Admin-Rechten definiert werden. Der li-admin-Benutzer muss sich von einem externen Server (von LEA) anmelden, um diese "Buffer"-Option zu aktivieren. Jeder andere Administrator-Benutzer, der versucht, sich im lokalen Kontext in den Knoten anzumelden, darf diese "Buffer"-Option nicht definieren.

Hier sind die Schritte, um die Anforderung für die "Buffer"-Option in StarOS unter LI-Modul zu erreichen.

1. Melden Sie sich mit dem lokalen Administrator-Benutzer beim Knoten an.
2. Erstellen Sie li Kontext (da es dort keinen dedizierten li Kontext gab).
3. Erstellen Sie li user mit li-admin Berechtigungen im lokalen Kontext.
4. Erstellen Sie li Benutzer mit li-admin Berechtigungen im li Kontext.
<<wir haben li-admin aus dem lokalen Kontext entfernt, um dedizierte li hinzuzufügen, sodass wir den li-Kontext vom lokalen Kontext trennen können **>>**
5. Entfernen Sie den Benutzer li mit der Berechtigung li-admin aus dem lokalen Kontext.
6. Erstellen Sie einen dedizierten li-Kontext, um die separate li-Konfiguration zu ermöglichen.
7. Definieren Sie die Zugriffsliste unter li Kontext.
8. Abmelden vom Knoten.
9. Melden Sie sich mit dem "li"-Benutzer, der als li-admin berechtigt ist, wieder beim Knoten an.
10. Konfigurieren Sie die Pufferoption, die erforderlich ist, es sollte Ihnen erlauben, sie zu konfigurieren.

Konfiguration

```
[local]<hostname>(config)# context local
[local]<hostname>(config-ctx)# administrator li-admin password *** li-administration ftp
[local]<hostname>(config-ctx)# end

[local]<hostname>(config)# context li
[li]<hostname>(config-ctx)# administrator li-admin password *** ftp li-administration

<we removed li-admin from local context to add dedicated li which will help us to enable the
segregate the li context from local context >

[local]<hostname>(config-ctx)# no administrator li-admin
[local]<hostname>(config-ctx)# exit
```

```
[local]<hostname>(config)# dedicated-li context li
Warning: Creating a dedicated LI context is a permanent configuration setting
Info: Context li is dedicated to Lawful-Intercept configuration
Info: Undefined ACLs will be set to deny-all within this context
[li]<hostname>(config-ctx)#
[li]<hostname>(config-ctx)# access-list undefined permit-all
[li]<hostname>(config-ctx)# end
```

Nachdem Sie sich beispielsweise mit dem Benutzer li-admin angemeldet haben, können Sie alle benötigten Optionen sehen:

```
<local-node><hostname>$ ssh li-admin@li@
```

```
Cisco Systems QvPC-SI Intelligent Mobile Gateway
li-admin@li@aa.bb.cc.dd's password:
Last login: Wed Jan 23 17:32:31 -0500 2019 on pts/2 from 10.xx.yy.zz.
Cisco Systems QvPC-SI
Lawful Intercept Interface

No entry for terminal type "xterm-256color";
using dumb terminal settings.
[li] # configure
Warning: One or more other administrators may be configuring this system
[li]
```

buffer - This is used to configure the LI buffering >>>>>>> **We can see the buffer option now.**
dest-addr - Destination IP address where the intercepted information needs to be forwarded.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.