

2.2.15 Ensure mail transfer agent is configured for local-only mode (Scored)

Profile Applicability

```
Level 1 - Server  
Level 1 - Workstation
```

Description

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Audit

Run the following command and verify that the MTA is not listening on any non-loopback address (127.0.0.1 or ::1):

```
# netstat -an | grep LIST | grep ":25[[:space:]]"  
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
```

Remediation

Edit /etc/postfix/main.cf and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = localhost
```

Restart postfix:

```
# service postfix restart
```

Notes

This recommendation is designed around the postfix mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/ubuntu1604/2/2/15>

Last update: **2017/05/02 10:59**

