Product Notice #0255

Best Practice for System Resource Management on MSBR Devices

Notice Subject

Best practice for disabling management servers on MSBR devices to avoid an overload of operating system resources.

Notice Date

September 16, 2015

Notice Effective Date

Immediate

Affected Product Family

Mediant MSBR series running formal releases between **6.80A.269.011** until **6.80A.281.004** (including 281.004).

Notice Details

When a management server (Web, Telnet and SSH servers) that is running on an MSBR device is completely disabled, this can under certain circumstances lead to an improper release of file descriptors that are used by the operating system for various tasks. This consequently leads to a system resource overload and may cause units to be unresponsive when running specific services.

Problem Description

Units with any of the above mentioned Management servers disabled using the CLI commands shown below, may be affected, depending on other configuration parameters (such as firewall and access lists on the network interfaces):

- **telnet disable:** command for disabling Telnet server (under configure system, cli)
- **ssh off:** command for disabling SSH server default value (under configure system, cli)
- **secure-connection on:** command for disabling HTTP server (under configure system, web)

AudioCodes Inc.
27 World's Fair Drive, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O. Box 255, Ben Gurion Airport, Israel, 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/info
Website: www.audiocodes.com

Corrective Actions

Perform one of the following actions to prevent this problem occurring:

- Upgrade units to versions running firmware equal or greater than **6.80A.285.001**.
- Perform the configuration described below for units running firmware version **6.80A.269.011** until version **6.80A.281.004**.

Note: It is strongly recommended to perform the following configuration to disable management servers for the above listed versions.

Do the following:

1. Enter the following command for all Management servers:

```
conf data
access-list DISABLE-SERVICE deny ip any any
exit
```

2. Enter the following commands according to the relevant Management server:
   - Telnet:

```
conf system
cli
telnet-acl DISABLE-SERVICE
exit
exit
```

   - SSH:

```
conf system
cli
ssh-acl DISABLE-SERVICE
exit
exit
```

   - Web:

```
conf data
access-list DISABLE-WEB deny ip any an
exit

conf system
web
web-acl DISABLE-WEB
exit
exit
```

Note:

- Management access-lists match only the remote IP address with the source IP/mask in the rule set. These lists ignore any other information in the rules.
- The management access list for web is shared between HTTP and HTTPS. For users who must shutdown HTTP completely, and cannot define shared criteria with HTTPS, access-lists can be attached to the network interfaces, thereby blocking the HTTP port. See example CLI commands below:

```
access-list MGMT deny tcp any local eq 80
access-list MGMT permit ip any any

interface GigabitEthernet 0/0
ip access-group MGMT in
```