Cisco BAC 3.6 Hardening Guidelines

The Cisco BAC 3.6 hardening guide describes the procedure to harden your system while running Cisco Broadband Access Center (Cisco BAC) 3.6:

Overview

The hardening guidelines help you to identify and eliminate any security vulnerabilities pertaining to Cisco BAC 3.6 and its supporting software and hardware components. These guidelines also include information on protocol robustness, which defines the application stamina when exposed to Denial-of-Service attacks and protocol irregularities.

For Cisco BAC 3.6, the hardening guidelines are defined and tested using 5.10 Generic_137111-04 sun4u sparc SUNW, Sun-Fire-V215 hardened with Solaris Security Toolkit 4.2.

We recommend that you harden your systems to mitigate security threats while deploying the Cisco BAC 3.6.

Note: Complying with these hardening guidelines does not guarantee the elimination of all security threats. However, by implementing these guidelines, you can achieve a higher-level of security and help manage unforeseen risks.

Hardening Your System

To harden your system you must follow these steps:

1. Ensure that all the Sun Microsystems recommended operating system and security patches have been installed on your system. Contact Sun Microsystems support to download the recommended patches and check for any applicable updates. You can check the patch details by running the following commands:

```
# uname -a
# showrev -p | grep PatchNumber
```

Where *PatchNumber* is the Solaris patch number.
Example:

```
# uname -a
SunOS SecuredSunHost 5.10 Generic_137111-04 sun4u sparc SUNW, Sun-Fire-V215

# showrev -p | grep 137111-04
Patch: 137111-04 Obsoletes: 138052-01, 138054-01, 138315-01, 138316-01 Requires:
118833-36, 119578-30, 120011-14, 126897-02, 127127-11, 127755-01 Incompatibles:
Packages: SUNWcsu, SUNWcsr, SUNWcsl, SUNWkvm, SUNWcakr, SUNWckr, SUNWcsd, SUNWfmd,
SUNWesu, SUNWmdb, SUNWmdbr, SUNWtoo, SUNWcslr, SUNWarcr, SUNWdtrc, SUNWhea
```

2. Disable unused network services. All network services can be disabled except the secure shell by using the following command:

```
# netservices limited
```

Example:

```
# netservices limited
restarting syslogd
restarting sendmail
restarting wbem
dtlogin needs to be restarted. Restart now? [Y] y
restarting dtlogin
```

3. Change to the directory that contains the Sun Solaris Security Toolkit package and install the package (SUNWjass) by using the following command:

```
# pkgadd -d ./
```

Example:

```
# pkgadd -d ./
The following packages are available:
  1  SUNWjass     Solaris Security Toolkit 4.2.0
                  (Solaris) 4.2.0
Select package(s) you wish to process (or 'all' to process all packages). (default:
all) [?,??,q]:

Processing package instance <SUNWjass> from </opt>

Solaris Security Toolkit 4.2.0(Solaris) 4.2.0
Copyright 2005 Sun Microsystems, Inc.  All rights reserved.
Use is subject to license terms.

Using </opt> as the package base directory.
## Processing package information.
## Processing system information.
   415 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

Installing Solaris Security Toolkit 4.2.0 as <SUNWjass>

## Installing part 1 of 1.
[ verifying class <none> ]

Installation of <SUNWjass> was successful.
```

4. Disable unused daemons and services, especially services that use network resources. The following is an example on how to disable services:

```
# svcadm disable svc:/network/smtp:sendmail
# svcadm disable svc:/network/finger:default
```

5. Uninstall all unused applications.
6. Apply the highest-level of password protection to all network applications and services. Ensure that you change the default passwords.
7. Use HTTPS to access the Cisco BAC administrator user interface and disable the HTTP access. The HTTP access to the administrator user interface (using port 80) is enabled by default on the RDU. You cannot disable the HTTP service using standard Cisco BAC administrative methods. However, you can disable the HTTP access using the Tomcat *server.xml* file, which is located at *BPR_HOME*/rdu/tomcat/conf (*BPR_HOME* is the Cisco BAC installation directory). To disable the HTTP access, do the following:
   a. Comment out the HTTP/80 connector directive in the Tomcat server.xml file. For example:

```
<!--    <Connector port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="443" />
-->
```

   b. Reload the Tomcat process to make your changes take effect:

```
# /etc/init.d/bprAgent restart tomcat
Process [tomcat] has been restarted.
```

8. Shut down the SNMP service, if it is not used to manage the Cisco BAC components. The SNMP service is enabled by default on the RDU and DPEs, and it uses UDP port 8001. You can disable this service on the RDU or DPE by running the following command from the *BPR_HOME*/snmp/bin:

```
# ./snmpAgentCfgUtil.sh stop

Process [snmpAgent] has stopped.
```

Note: Do not run `snmpAgentCfgUtil.sh`, if you are using SNMP service.

Cisco BAC 3.6 supports TACACS+ feature. The user login was tested with TACACS+ server and local login.

Product Documentation

The following documents provide detailed information about installing and using Cisco BAC 3.6:

- Release Notes for Cisco Broadband Access Center, Release 3.6
- Installation Guide for Cisco Broadband Access Center, Release 3.6
- Cisco Broadband Access Center Administrator's Guide, Release 3.6
- Integration Developer's Guide for Cisco Broadband Access Center, Release 3.6
- Cisco Broadband Access Center DPE CLI Reference, Release 3.6
- Cisco Broadband Access Center 3.6 Third Party and Open Source Copyrights

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.