Operating System and Security Hardening

Security Hardening

We provide the following overview of security features in Unified Communications Manager 12.5SU3. Some of the items below are prior to the availability of planned updates to Cisco's standard product documentation.

Unified Communications Manager runs as a virtual machine on top of virtualized hardware based on VMware vSphere ESXi. Unlike conventional server-based products, Unified Communications Manager is a software product distributed as a closed-system, turnkey-packaged, "appliance" workload, which:

- Reduces the attack surface
- Provides a more stable, higher performance configuration
- Avoids vulnerabilities from configuration errors
- Simplifies administration and corrective maintenance without requiring OS / DB skill sets

Highlights of Unified Communications Manager workload-layer hardening include:

- Unified Communications Manager isn't a general-purpose / open-system workload.
  - It doesn't use a general-purpose OS distribution.
    - Unused modules are excluded from the image and unused services are disabled / removed.
    - We make proprietary hardening changes to specific modules (for example, OpenSSL is hardened by Cisco's Security and Trust Organization; the resulting CiscoSSL is incorporated into the product).
  - Native interfaces to guest Operating System, Database, runtime, and other workload software components are not exposed.
    - They are either removed or hidden and locked-down.
    - Access is only through Cisco-provided browser-based GUI, CLI, or API, with various mechanisms to secure those interfaces (e.g., CLI via SSH, or pull files into workload via Secure FTP).

- The product comprises a carefully controlled stack that contains all software required to operate, maintain, secure, and manage the application. We specify, install and update all this software through images provided and digitally signed by Cisco.
- All of the above information are subject to the development and test processes of the Cisco Secure Product Lifecycle development approach, as described here: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

- The Unified Communications Manager workload layer does not support insertion of non-Cisco software or software updates/changes outside the above-mentioned controlled Cisco-provided interfaces.
  - All software within the workload is provided by Cisco and digitally signed and delivered as a monolithic image (.ISO file).
  - The only way to install, upgrade and update software is by using a Cisco-provided .ISO or .COP file.
  - .ISO file installs or updates one, some, or all of the software elements in the Cisco image .COP files are used to update single elements, most commonly user locales and phone firmware updates.
  - The following are not enabled or possible:
    - onboard agents like anti-virus clients, UPS agents, management agents and so on.
    - customer-uploadable or externally-uploadable software.
    - 3rd-party applications.

- “Root access” to the guest OS inside the workload is not enabled:
  - Customers use authentication in the Cisco-provided GUI, CLI, and/or API.
  - All exposed interfaces to the workload are secured (e.g., enforced password complexity rules, SSH instead of telnet, TLS 1.2 with configurable minimum version and so on.)
  - For emergency issues that are not fixable in the field thru the normal GUI/CLI/API, customers can set up a temporary "Remote Account" so that a Cisco Technical Assistance Center (TAC) expert can gain root access. The customer maintain controls and can turn on or turn off this account with auto-expiry. The customer can see what the TAC representative is doing with all actions being performed by TAC being logged.

- Built-in Intrusion Prevention Capabilities:
  - SELinux enforcing mode, providing host-based intrusion protection.
    - SELinux enforcing mode is enabled by default. This mode enforces mandatory access controls that confine applications, daemons, etc. to the “least privilege” required to do their job.
  - IPTables host-based firewall:
    - IPTables is enabled by default.
    - The rules are adjusted by Cisco Service Activation to open the appropriate ports and include the correct rate limiting for the services being used on that server.
    - The IPTable rules can be displayed using the following commands:
      - **utils firewall ipv4 list**

- **utils firewall ipv6 list**

In addition to the above hardening features, Unified Communications Manager workload performs security audit logging for OS, DB and application software. There are three security audit logs included:

- Linux auditd log.
- Unified CM Application audit log.
- Informix database audit log.

There are also configuration settings that allow the system administrator to configure the system to comply with the organization's infosec requirements. The system administrator-configurable security settings and utilities include, but are not limited to:

- Defining password policies. All passwords and PINs are hashed or encrypted and not stored as clear text.
- Account lockout settings and credential policy.
- Warning banner text.
- Enabling TLS/SRTP for signaling and media.
- Phone hardening settings.
- IPSec to secure connections which do not use TLS.
- Changing the self-signed PKI certificates to CA signed.
- Enabling FIPS mode or Common Criteria mode.
- Enabling SAML Single Sign-On which includes support for smart cards or bio-metric readers.
- View all network connections, processes, active packages.
    - "show network status detail all nodns" Retrieves details on open ports, equivalent to a "netstat -an" Unix command.
    - "show process list detail" Retrieves a list of all the processes and critical information about each process, equivalent to a "ps -ef" Unix command.
    - "show packages active" Displays the name and version for installed and active packages.

More details on configurable security options are in the Security Guide for Cisco Unified Communications Manager.

Cisco's UC offerings are regularly tested and validated to be compliant with a range of government certifications, including:

- Department of Defense Information Network Approved Products List (DoDIN APL)
- FIPS 140-2 Level 1
- FedRAMP
- Common Criteria
- Applicable U.S. Department of Defense Security Technical Implementation Guides (STIGs)

For additional information on Cisco government certifications, see https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html

For security vulnerability alerts and management, the entire Unified Communications Manager workload falls under the umbrella of the Cisco Product Security Incident Response Team (PSIRT). Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products. You should:

- Monitor the Cisco Security Advisories and Alerts page (https://tools.cisco.com/security/center/publicationListing.x) for alerts concerning security issues that may affect your deployment.
- View the Cisco.com security advisory page for a given PSIRT to learn affected products, workarounds, and permanent fixes.

For more information, see: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html