VULNERABILITY REPORT

Auditing vulnerabilities in network Cisco devices.

Customer

Tuya

support@vulnapp.co
www.vulnapp.co

05/11/2017

1. SUMMARY

1.1. Introduction

VulnAPP performed a security audit on 05/11/2017 of the device detailed in the next table.

Security audit device list		
Device	**Name**	**OS**
Cisco	Router	12.42

1.2. Security Issue Overview

Each security issue identified by VulnAPP is described with a finding, the impact of the issue, how easy it would be for an attacker to exploit the issue and a recommendation.

Issue published date: date when the vulnerability was publicly available.

Issue description: the issue finding describes what VulnAPP identified during the security audit. Typically, the finding will include background information on what particular configuration settings are prior to describing what was found.

Issue impact: the issue impact describes what an attacker could achieve from exploiting the security audit finding. However, it is worth noting that the impact of an issue can often be influenced by other configuration settings, which could heighten or partially mitigate the issue. For example, a weak password could be partially mitigated if the access gained from using it is restricted in some way.

Issue recommendation: each issue includes a recommendation section which describes the steps that VulnAPP recommends should be taken in order to mitigate the issue. The recommendation includes, where relevant, the commands that can be used to resolve the issue.

Issue affected products: the software version that are vulnerable to the issue.

Issue references: links about additional information of the issue and workarounds.

1.3. Rating System Overview

Each issue identified in the security audit is rated against both the impact of the issue and how easy it would be for an attacker to exploit. The fix rating provides a guide to the effort required to resolve the issue. The overall rating for the issue is calculated based on the issue's impact and ease ratings.

Impact Rating

An issue's impact rating is determined using the criteria outlined in the next table:

The impact rating	
Rating	**Description**
CRITICAL	These issues can pose a very significant security threat. The issues that have a critical impact are typically those that would allow an attacker to gain full administrative access to the device. For a firewall device, allowing all traffic to pass through the device unfiltered would receive this rating as filtering traffic to protect other devices is the primary purpose of a firewall.
HIGH	These issues pose a significant threat to security, but have some limitations on the extent to which they can be abused. User level access to a device and a DoS vulnerability in a critical service would fall into this category. A firewall device that allowed significant unfiltered access, such as allowing entire subnets through or not filtering in all directions, would fall into this category. A router that allows significant modification of its routing configuration would also fall into this category.
MEDIUM	These issues have significant limitations on the direct impact they can cause. Typically, these issues would include significant information leakage issues, less significant DoS issues or those that provide significantly limited access. An SNMP service that is secured with a default or a dictionary-based community string would typically fall into this rating, as would a firewall that allows unfiltered access to a range of services on a device.
LOW	These issues represent a low level security threat. A typical issue would involve information leakage that could be useful to an attacker, such as a list of users or version details. A non-firewall device that was configured with weak network filtering would fall into this category.

2. Findings

Cisco IOS Software and IOS XE Software TCP Packet TCP packet memory leak Vulnerability

CVE-2015-0646

Published Date: 2015 Mar 25

Impact: HIGH

Description: a vulnerability in the TCP input module of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak and eventual reload of the affected device.

The vulnerability is due to improper handling of certain crafted packet sequences used in establishing a TCP three-way handshake. An attacker could exploit this vulnerability by sending a crafted sequence of TCP packets while establishing a three-way handshake. A successful exploit could allow the attacker to cause a memory leak and eventual reload of the affected device.

Recommendation: There are no workarounds for this vulnerability.
Cisco has released software updates that address this vulnerability. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

Affected Products:
Cisco devices that are running affected Cisco IOS Software (<15.2) or Cisco IOS XE Software are vulnerable. Cisco devices running Cisco IOS or Cisco IOS XE Software configured with any process listening on any TCP port are potentially affected. There are multiple processes in Cisco IOS Software that can be configured to listen on TCP ports. Examples of such configured processes are HTTP, HTTPS, SSH, or Telnet. Other configured processes may exist on an affected device and may listen on TCP ports. The configuration necessary to determine whether any of the TCP listening processes is enabled on a Cisco device is specific to the configured process.

On certain devices running Cisco IOS and Cisco IOS XE Software it is possible to determine if any processes are listening on TCP ports. To determine whether a Cisco IOS device or Cisco IOS XE device would process TCP packets destined to a listening service, log into the device and issue either of the following command line interface (CLI) commands show tcp brief all, or show control-plane host open-ports. If the output shows any process listening on any TCP ports, the device is vulnerable.

References:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak
https://nvd.nist.gov/vuln/detail/CVE-2015-0646

Cisco IOS Software Tunnels Vulnerability

CVE-2009-2872, CVE-2009-2873

Published Date: 2009 Sep 23

Impact: High

Description: Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.

Cisco Express Forwarding is a Layer 3 IP switching technology. It improves network performance and scalability for networks with high and dynamic traffic patterns.

Recommendation:

- Disabling Cisco Express Forwarding will mitigate this vulnerability.
- Cisco Express Forwarding can be globally disabled by using the no ip cef and no ipv6 cef global configuration commands

Affected Products:
Devices that are running Cisco IOS Software (<12.4(23)) and configured for GRE, IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels tunnels and Cisco Express Forwarding may reload upon switching a specially crafted malformed packet. Please note that using PPTP creates GRE tunnels that are transparent to the end user so devices configured for PPTP are vulnerable if they are configured on an affected software version. Using MVPN also creates GRE tunnels that are transparent to the end user. However, MVPN configurations are not vulnerable.

References:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels
https://nvd.nist.gov/vuln/detail/CVE-2009-2872

TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products

CVE-2008-4609

Published Date: 2009 Sep 08

Impact: High

Description: multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

Recommendation VulnApp:

- Cisco IOS Software
- The Cisco Guide to Harden Cisco IOS Devices provides examples of many useful techniques to mitigate against the TCP state manipulation vulnerabilities. These include:
- Infrastructure Access Control Lists (iACL)
- Receive Access Control Lists (rACL)
- Transit Access Control Lists (tACL)
- VTY Access Control Lists
- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)
- Management Plane Policing (MPP)
- For more information on the topics listed above, consult the Cisco Guide to Harden Cisco IOS Devices at the following link: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Affected Products:

- Cisco IOS Software
- Cisco IOS-XE Software
- Cisco CatOS Software

- Cisco NX-OS Software
- Linksys Products
- Scientific Atlanta Products

References:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24
https://nvd.nist.gov/vuln/detail/CVE-2008-4609

Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability

CVE-2009-0631

Published Date: 2009 Mar 25

Impact: High

Description: several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Recommendation:

- VulnApp recommends:
- Disable Affected Listening Ports
- If an affected feature is not required, it can be explicitly disabled. Once disabled confirm the listening UDP port has been closed by entering the CLI command "show udp" or "show ip socket". Some features may require a reload of the device after disabling the feature in order to close the listening UDP port.
- For SIP it is possible to disable UDP listening if only TCP services are required. The following example shows how to disable SIP from listening on its associated UDP port.
- Check more workarounds in the next link:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

Affected Products:

- Devices running affected versions of Cisco IOS Software (<12.4(23)) and Cisco IOS XE Software

- IP Service Level Agreements (SLA) Responder
- Session Initiation Protocol (SIP)
- H.323 Annex E Call Signaling Transport
- Media Gateway Control Protocol (MGCP)

References:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp
https://nvd.nist.gov/vuln/detail/CVE-2009-0631

RIP routing protocol: Version 1 enabled

Impact: High

Description:
RIP is a routing protocol that allows network devices to dynamically adapt to changes in the network infrastructure. There are three main versions of RIP:

Version 1 of the protocol, outlined in RFC 1058, supports simple routing updates with support only for classful routing and broadcast updates;

Version 2 of the protocol, outlined in RFC 2453, added support for Classless Inter-Domain Routing (CIDR), authentication (both in clear-text and MD5 forms) and multicast updates;

NG, outlined in RFC 2080, adds support for Internet Protocol version 6 (IPv6) but does not include support for authentication.

Recommendation:
- VulnApp recommends that, if RIP is required, only support for version 2 should be configured. However, this may require a firmware update if the device does not support version 2.
- Support for only RIP version 2 updates can be configured on Cisco Router devices with the following router configuration command:

version 2

- Additionally, RIP version 2 support can be configured on individual interfaces with the following interface commands:

ip rip send version 2

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfrip.html

Clear-text SNMP in Use

Impact: High

Description: SNMP is an industry standard protocol for monitoring and managing a variety of devices. SNMP services typically offer detailed information that includes a device's operating system, network interfaces, memory, system counters and system users. With write access to SNMP, it is possible to re-configure networking, system properties and even shutdown a device.

There are multiple versions of SNMP and versions prior to version 3 offer no encryption of either the authentication or data network traffic.

VulnApp determined that the clear-text SNMP versions were enabled om the device.

Recommendation:

- VulnApp recommends that, if not required, SNMP should be disabled. However, if SNMP access is required, VunApp recommends that only SNMP version 3 should be configured with strong authentication and privacy passwords.
- SNMP can be disabled with the following command:
-

no snmp-server

Affected products: The vulnerability affects to Cisco products that have enabled SNMP version 1 and 2c.

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html

Enabled password Configured

Impact: High

An attacker who had access to the Cisco configuration file would easily be able to retrieve passwords that are stored in clear-text or using the Cisco type-7 encryption. However, an attacker who had access to a Cisco configuration file could attempt a brute-force attack against the stronger MD5 hashes. Tools can be downloaded from the Internet that are capable of reversing Cisco Type 7 passwords. However, an attacker would need to obtain a copy of the configuration file and would need to be able to gain initial access to the device before they could make use of an enable password.

Description: Cisco Internet Operating System (IOS)-based devices enable passwords can be stored using MD5 hashes or using the Cisco Type 7 password encoding algorithm. A strong password stored using an MD5 hash can take a significant period of time to brute-force. However, the same password stored in Cisco Type 7 form can be reversed in a fraction of a second. The MD5 enable user password hash can be created using the secret keyword, whilst the Cisco Type 7 hash is created using the password keyword.

Recommendation:

- VulnApp recommends that all enable passwords should be stored using the MD5 hash. The following command can be used to remove the Cisco Type 7 enable password.

```
no enable password
```

- MD5 enable passwords can be configured using the following command:
-

```
enable secret [level password] password
```

Affected products
The vulnerability affects all Cisco products that have "enable password" activated.

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

UDP Small Services Enabled

Impact: High

Description: Some devices and platforms provide a collection of simple User Datagram Protocol (UDP) network services, which are also sometimes referred to as small services. These services provide little functionality and are rarely used and they typically include:

Discard (defined in RFC 863) ignores any data sent to it by a connecting client;
Chargen (defined in RFC 864) generates printable characters which are returned to the connecting client.

The vulnerability affects to Cisco products.

An attacker could use the UDP small servers as part of a DoS attack. UDP is a connection-less protocol and an experienced attacker could forge network packets to use the echo and chargen services to increase the network traffic and system utilization of devices offering the services. Additionally, each running service increases the chances of an attacker being able to identify the device and successfully compromise it. Although not as significant, some of the services may provide an attacker with simple information that could then be used as part of a targeted attack against the system.

Recommendation:

- VulnApp recommends that the UDP small servers should be disabled.
- UDP small servers can be disabled on Cisco Router devices with the following command:
-

no service udp-small-servers

References:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

SNMP Remote Code Execution Vulnerabilities in Cisco IOS XE Software

CVE-2017-6736
Impact: High

Published Date: 2017 Jun 29

Description: the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community

user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve57697.

Recommendation:

- Administrators are advised to allow only trusted users to have SNMP access on an affected system. Administrators are also advised to monitor affected systems by using the show snmp host command in the CLI.
- In addition, administrators can mitigate these vulnerabilities by disabling the following MIBs on a device:
- ADSL-LINE-MIB
- ALPS-MIB
- CISCO-ADSL-DMT-LINE-MIB
- CISCO-BSTUN-MIB
- CISCO-MAC-AUTH-BYPASS-MIB
- CISCO-SLB-EXT-MIB
- CISCO-VOICE-DNIS-MIB
- CISCO-VOICE-NUMBER-EXPANSION-MIB
- TN3270E-RT-MIB

Affected products
These vulnerabilities affect all releases of Cisco IOS and IOS XE Software prior to the first fixed release and they affect all versions of SNMP—Versions 1, 2c, and 3.

References:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp
https://nvd.nist.gov/vuln/detail/CVE-2017-6736

AUX Port Not Disabled

Impact: Medium

If an attacker is able to dial in and connect to the device remotely using the AUX port, the attacker could perform a brute-force attack against the authentication mechanism in order to gain remote administrative access. If a malicious user was able to gain physical access to a device where the AUX port had not been disabled, they could attach a modem in order to perform an attack from a remote location. If a callback

network administrators phone number.

Description: the Auxilary (AUX) port's primary purpose is to provide a remote administration capability. With a modem connected to the AUX port, a remote administrator could dial into the device in order to perform remote administration. As an extra layer of security, some devices can be configured with a callback facility. The callback facility, if configured, drops any incoming calls and dials the network administrator back.

Recommendation:

- VulnApp recommends that, if not required, the AUX port should be disabled. If the AUX port is required and the device supports callback then VulnApp suggests that the callback facility should be configured as an additional level of protection.
- The auxiliary port can be disabled with the following IOS auxiliary line commands:
-

transport input none
login local
no exec

Affected products: The vulnerability affects all Cisco products that have Auxiliary port enabled.

References:
https://www.cisco.com/c/en/us/support/docs/routers/1600-series-routers/46789-port-pinout.html

Login Password Retry Lockout

Impact: Medium

Description: the Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in using the username that corresponds to the AAA user account. A locked-out user cannot successfully log in again until the user account is unlocked by the administrator.

A system message is generated when a user is either locked by the system or unlocked by the system administrator. The following is an example of such a system message:

%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.

Recommendation: VulnApp recommends to configure the Login Password Retry Lockout feature, perform the following steps.

SUMMARY STEPS
1. *enable*
2. *configure terminal*
3. *username name [privilege level] password encryption-type password*
4. *aaa new-model*
5. *aaa local authentication attempts max-fail number-of-unsuccessful-attempts*
6. *aaa authentication login default method*

Affected products: the vulnerability affects to Cisco products that have not enabled aaa model and limit for unsuccessful-attempts.

References:
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-login-pw-retry.html

No Inbound TCP Connection Keep-Alives

Impact: Medium

An attacker could attempt a DoS attack against a device by exhausting the number of possible connections. To perform this attack, the attacker could keep requesting new connections to the device and spoof the source IP addresses. This would then prevent any new legitimate connections to the device from being made as the device awaits the completion of the connection attempts that have already been initiated. This attack would prevent both users and administrators from connecting to the device.

Description: the keep-alive messages are used to determine if a connection is active or has become orphaned and is no longer used. Depending on the result, the device can reclaim resources allocated to inbound connections that have become orphaned. Connections to a device could become orphaned if a connection becomes disrupted or if the client has not properly terminated a connection.

Recommendation:

VulnApp recommends that TCP keep alive messages should be sent to detect and drop orphaned connections from remote systems.

command:

service tcp-keepalives-in

Affected products: the vulnerability affects to Cisco products.

References:
https://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/14957-tcpkeepalive.html

Syslog Logging Not Enabled

Impact: Medium

If logging of system messages is not configured, a network administrator may not be made aware of significant events happening on the device. These events could include security issues such as intrusion attempts, network scans, authentication failures or diagnostic and management information such as potential hardware issues. Without logging system messages, the information would not be available to either a forensic investigation or for diagnostic purposes.

Description: logging is an important component of a secure network configuration. When appropriately configured, the messages logged provide a wealth of information to a network administrator when diagnosing a problem, identifying an attack or when used to provide an activity audit trail. When a well configured logging system is combined with a good monitoring and alert system it will enable network administrators to promptly respond to networking issues, DoS attacks, administrative system logons and a host of other important information.

Syslog logging provides an industry standard system (detailed in RFC 5424) for logging messages, enabling the collection, storage and administration of logs from a variety of devices to a single location. The sending of logs to other systems, not only provides extra storage space for logs which could be size restricted on the originating network device, but it also provides an extra level of protection for the logs in a scenario where an attacker has compromised the security of the message sourceLogging is an important component of a secure network configuration. When appropriately configured, the messages logged provide a wealth of information to a network administrator when diagnosing a problem, identifying an attack or when used to provide an activity audit trail. When a well configured logging system is combined with a good monitoring and alert system it will enable network administrators to promptly respond to networking issues, DoS attacks, administrative system logons and a host of other important information.

enabling the collection, storage and administration of logs from a variety of devices to a single location. The sending of logs to other systems, not only provides extra storage space for logs which could be size restricted on the originating network device, but it also provides an extra level of protection for the logs in a scenario where an attacker has compromised the security of the message source.

Recommendation:

VulnApp recommends that Syslog logging should be configured to enable system messages to be logged to a central logging server.
Notes for Cisco Router devices:
The logging of system messages to a remote Syslog host can be configured using the following command:

logging host ip-address

Affected products: The vulnerability affects to all Cisco products that has not set up a external syslog server.

References:
https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html

Clear Text HTTP Service Enabled

Impact: Medium

Due to the lack of encryption provided by the HTTP service, an attacker who is able to monitor a session would be able to view all of the authentication credentials and data passed in the session. The attacker could then attempt to gain access to the device using the authentication credentials extracted from the session and potentially gain access under the context of that user. Since HTTP is commonly used for network device administration this could gain the attacker an administrative level of access.

Description: HTTP (RFC 2616) provides web-based services, such as information services, network device administration and other potentially sensitive services. HTTP provides no encryption of the connection between the client and server including any authentication and data transfer.

Recommendation:

VulnApp recommends that the HTTP service should be disabled. If remote administrative access is required then VulnAPP recommends that a cryptographically secure alternative, such as HTTPS, should be used

The HTTP server can be disabled using the following command:

no ip http server

Affected products: the vulnerability affects to all Cisco products.

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/12-2sy/https-12-2sy-book/nm-http-web.html

Multiple Vulnerabilities in ntpd (April 2015) Affecting Products

CVE-2015-1799

Impact: Medium

Description: Multiple Cisco products incorporate a version of the ntpd package. Versions of this package are affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to bypass authentication controls or to create a denial of service (DoS) condition.

On April 7, 2015, NTP.org and US-CERT released a security advisory dealing with two issues regarding bypass of authentication controls. These vulnerabilities are referenced in this document as follows:

CVE-2015-1798: NTP Authentication bypass vulnerability
CVE-2015-1799: NTP Authentication doesn't protect symmetric associations against DoS attacks

Cisco has released software updates that address these vulnerabilities.

Recommendation: Limiting access to NTP hosts to only trusted sources will reduce the risk of exploitation. An attacker could exploit these vulnerabilities using spoofed packets.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link:

http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=36857

Affected products: Check in the next link, the products and services affected for this vulnerability:

References:
https://nvd.nist.gov/vuln/detail/CVE-2015-1799
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150408-ntpd

No Warning In Pre-Logon Banner

Impact: Low

A carefully worded warning message could deter a casual attacker or malicious user, but not a determined attacker. However, it would be more difficult to prove any intent without a message warning against unauthorized access if any legal action were to be taken against an attacker.

Description: logon banner messages are an important, but often overlooked, part of a secure configuration. Logon banner messages can provide connecting users with important information and warn against unauthorized access.

Recommendation:

VulnApp recommends that all pre-logon banner messages should be configured to warn against unauthorized access.
Notes for Cisco Router devices:
The Login banner message is presented to users before they logon to Cisco Router devices and after the Message Of The Day (MOTD) message is shown on Telnet connections. The Login banner message can be configured using the following command:

banner login delimiter banner-message delimiter

Affected products: The vulnerability affects to all Cisco products.

References: https://learningnetwork.cisco.com/thread/73815

CDP Was Enabled

Impact: Low

CDP packets contain information about the sender, such as hardware model information, operating system version and IP address details. This information would give an attacker valuable information about the device. The attacker could then use this information as part of a targeted attack.

Description: CDP is a proprietary protocol that was developed and is primarily used by Cisco. A CDP enabled device can be configured to broadcast CDP packets on the network enabling network management applications and CDP aware devices to identify each other. CDP packets include information about the sender, such as OS version and IP address information

Recommendation: VulnApp recommends that, if not required, CDP should be disabled.

In some configurations with IP phones, deployed using either Auto Discovery or Dynamic Host Configuration Protocol (DHCP), the CDP service may need to be enabled. However, if the device supports disabling CDP on individual interfaces, then VulnAPP recommends that it should be disabled on all the interfaces where it is not required.

Notes for Cisco Router devices:

The following commands can be used to disable CDP on Cisco Router devices. The first command disables CDP for the entire device, whilst the second can be used to disable CDP on individual interfaces.

```
no cdp run
no cdp enable
```

Affected products: The vulnerability affects to all Cisco products.

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf015.html