**Cisco Discovery Protocol Spoofing**

**Other names: CDP spoofing**

**Description 1**

CDP packets are enabled on all interfaces by default on Cisco switches and they are transmitted in clear text which allows an attacker to analyze the packets and create forged CDP packets and **gain a wealth of information about the network device then the attacker can use this information to execute a known vulnerability against the device platform**. [1]

**Description 2**

CDP contains information about the network device, such as the software version, IP address, platform, capabilities, and the native VLAN. When this information is available to an attacker computer, the attacker from that computer can use it to find exploits to attack your network, **usually in the form of a Denial of Service (DoS)** attack.

an attacker could spoof CDP packets and have them received by the attacker’s directly connected Cisco device. If the attacker can get access to the router either via Telnet or SNMP, they can use the CDP information **to discover the entire topology of your network at Layer 2 and 3, including all IOS levels, router and switch model types, and IP addressing**. If somebody was armed with this information and a Cisco bug list, they could launch a very effective attack against your network. [2]

**Description 3**

CDP spoofing is a technique employed tocompromise the operation of network devices that use the Cisco Discovery Protocol for discovering neighboring devices. CDP may be used between Cisco routers, switches and other network equipment to advertise their software version, capabilities and IP address. CDP spoofing is the creation of forged CDP packets that impersonate other devices, either real or arbitrary.

When a router running CDP receives a CDP packet, it begins to build a table that shows the neighboring devices discovered. An attacker can exploit this functionality by sending thousands of spoofed CDP packets to 01:00:0C:CC:CC:CC to fill neighbor tables in any devices on the network running CDP. When this happens, **other traffic on the network may be dropped as the device does not have the resources necessary to route it**. The **device's command line interface may also become unresponsive making it difficult to disable CDP during an ongoing attack**. [3]

**Reference**

**[1]** [**http://www.cisco.com/c/dam/en\_us/training-events/le31/le46/cln/promo/share\_the\_wealth\_contest/finalists/Hany\_EL\_Mokadem\_Switch\_Attacks\_and\_Countermeasures.pdf**](http://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf)

**[2]** [**https://howdoesinternetwork.com/2011/cdp-attack**](https://howdoesinternetwork.com/2011/cdp-attack)

**[3]** [**https://en.wikipedia.org/wiki/CDP\_Spoofing**](https://en.wikipedia.org/wiki/CDP_Spoofing)