WootCloud Detected Thousands of Exposed Cisco Routers Administrative Web Consoles

## Overview

WootCloud conducted an analytical study of exposed Cisco router devices on the Internet. The purpose of the study was to determine the potential number of exposed Cisco routers running administrative web consoles configured as a result of level 15 access. Exposed routers could become potential targets for malware authors to compromise these devices and use the same for nefarious purposes on the Internet by forming botnets. Compromised routers can be used for building botnets to trigger unauthorized operations such as launching brute-force attacks, bitcoin mining, building hidden proxy tunnels, and many others. The study reflects the risk carried by organizations for allowing the administrative web consoles to be exposed on the Internet that can be accessible by remote users without any restriction. In this research, WootCloud observed more than 200,000 Cisco routers running with exposed web administrative panels.

## Analysis

Any exposed cisco router running web service on TCP port 80 or TCP port 443 respectively send HTTP response headers as shown below:

```
HTTP/1.1 401 Unauthorized

Date: <Truncated>
Server: cisco-IOS
Connection: close
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15 or view access"
```

- The "Server" HTTP response header discloses the type of server used. It contains the information about the software used by the origin server to handle the request. Cisco router sends the value as "cisco-IOS" for the "Server" response header.
- The "WWW-Authenticate" HTTP response header defines the authentication method that should be used to gain access to a resource. Usually, the WWW-Authenticate header sent

along with a 401 Unauthorized response. Cisco router sends the value as “level_15 or view_access” for the “WWW-Authenticate:” response header.

As highlighted in the Cisco documentation, Cisco routers have three different privileges mode:

- Level 0 allows only five commands—Logout, enable, disable, help, and exit
- Level 1 provides minimal access to router functionality, e. read-only access
- Level 15 provides complete control of the router

An example of the exposed web administrative interface configured with level 15 access is shown below:

Access to the compromised router via level 15 is also shown below:

Another snapshot presented below highlighted the result of “/show/processes/CR” command executed via level 15 access via web interface.

The graph presented below shows the top 10 countries highlighting some exposed Cisco devices (routers) on the Internet that can be accessed by remote users.

Impacts

- Exposed web interface panels are susceptible to automated brute force attacks. If the Cisco router is not configured with an option “login block-for,” it gives a straightforward platform for the attackers to launch automated password cracking attack (or brute force) to gain access to the router.
- Web interface exposed and configured over non-HTTPS channel makes it vulnerable to Man-in-the-Middle (MitM) attacks on the same network. In this research, WootCloud observed the majority of the web administrative interfaces are available over the non-HTTPS

- The authentication prompt served by Cisco router web administrative uses HTTP basic authentication in which credentials are passed over the network as BASE64 encoded strings. Also, some HTTP requests require “Authorization” header to be transmitted that carry encoded credentials.
- Denial-of-Service (DoS) attacks can be triggered at layer 7 to abuse the web service thereby impacting the web functionality of the user.

Under the Common Weakness Enumeration (CWE) standards, some security weaknesses mapped to the existing study are shown below:

- Unprotected Primary Channel **https://cwe.mitre.org/data/definitions/419.html**
- Cleartext Transmission of Sensitive Information **https://cwe.mitre.org/data/definitions/319.html**
- Improper Restriction of Excessive Authentication Attempts **https://cwe.mitre.org/data/definitions/307.html**

Vulnerabilities

Some vulnerabilities highlighted below can be exploited by attackers to control the routers.

| | |
|---|---|
| Cisco Router Web Setup Ships with Insecure Default IOS Configuration | **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060712-crws** |
| Cisco IOS HTTP Server Vulnerability | **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20000514-ios-http-server** |
| Cisco IOS XE Software Web UI Privilege Escalation Vulnerability | **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-privesc** |
| IOS HTTP Authorization Vulnerability | **https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010627-ios-http-level** |

Countermeasures

Some countermeasures can be opted to restrict the exposure:

- Make sure only authorized sources to have access to web administrative panels

- Deploy security solution such as WootCloud to obtain continuous visibility into the IoT devices and analyzing the communication patterns accordingly
- As a proactive measure, scan external network perimeter to detect exposed devices