Internet Computing Solutions

Website Hosting & Design, Firewalls, Intrusion Detection, and Content Filtering

P.O. Box 1005, Greenwood, IN 46142, Phone: 317-886-8528, Fax: 866-571-0372

Vulnerability Scanning and Testing Report - Additional Notes
For Your Main FCU
TEST DATE: 01-01-2021

TCPIP Address: 10.1.10.11

IP ADDRES OWNER: The owner of the IP address is shown below from www.arin.net.

Full Name	**Comcast Cable Communications Inc**
Handle	**IC161-ARIN**
Email	**CNIPEO-Ip-registration@cable.comcast.com**
Telephone	**+1-856-317-7200**
Organization	**Comcast Cable Communications Inc**
Address	**1800 Bishops Gate Blvd** **Mount Laurel** **NJ** **08054** **United States**
Roles	**Administrative, Technical**

Net Range	**75.75.72.0 - 75.75.79.255**
CIDR	**75.75.72.0/21**
Name	**COMCAST-47**
Handle	**NET-75-75-72-0-1**
Parent	**NET-75-64-0-0-1**
Net Type	**ASSIGNMENT**
Registration	**Fri, 15 Oct 2010 14:00:19 GMT (Fri Oct 15 2010 local time)**
Last Changed	**Fri, 15 Oct 2010 14:00:19 GMT (Fri Oct 15 2010 local time)**

REPORT INFORMATION:
The Scan came back with one major risks, two medium risks and with mostly informational only messages. (We suspect that the one critical risk 137702 is a false positive. However you should follow-up with your firewall vendor to be sure it is up to date. As always recommended, you should take steps to ensure that the BIOS and/or Management software running on this device is always updated to the latest available version. This particular firewall does NOT appear to be updated to the latest version of software. New Risks and Vulnerabilities are created every day. Please contact a qualified network support person to verify the version of software is updated and to document for you any open ports, redirection services, firewall rules, etc. Ensure that access to the management interface of your router is using strong password techniques as described by industry standards. Tips for creating strong passwords can be found here: https://msdn.microsoft.com/en-us/library/ms161962.aspx. If this or any device provides wifi access to your office, be sure to use at least WPA2 security with AES encryption for your wifi keys and keep the wifi access completely off your main network where your data resides. The new Vulnerabilities are: 137702, 35291, 94761, 136318, 138614, 149334.

137702 (1) - Treck TCP/IP stack multiple vulnerabilities. (Ripple20)
This test shows that there is a possibility that the device is affected by the Ripple20 vulnerability. . Ripple20 is a series of 19 zero-day vulnerabilities found in a widely used, low-level TCP/IP software library developed by Treck, Inc. Ripple20 was disclosed in June, 2020. These vulnerabilities potentially affect hundreds of millions of OT and IoT devices and includes multiple remote code execution (RCE) vulnerabilities. This vulnerability test was developed by JSOF (https://www.jsof-tech.com/). See website for more info. This test has been known to trigger false positives. We recommend making sure the firewall software is up to date. You may need to contact the firewall vendor for additional information regarding the Treck Vulnerability. See this site for more info on Treck network stack: https://treck.com/vulnerability-response-information/

35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm
This test shows that the remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. We recommend making sure the firewall software is up to date and that an updated SSL Certificate be used to access the firewall.

51192 (1) - SSL Certificate Cannot Be Trusted – Medium Risk
This test shows that there is a possibility that the SSL Certificate cannot be trusted. Most likely the SSL Certificate used on this device is Self-Signed, which is the case in many firewalls that use an https:// management interface. Although this is listed as a medium risk, it is most likely no risk if a Self-Signed SSL Cert is used. To mitigate this medium risk, a Fully Authorized SSL Certificate can be used, however, they can cost upwards of a few hundred dollars or more per year. The image below shows the encryption that is used when accessing the login page of the router.

57582 (1) - SSL Self-Signed Certificate – Medium Risk
This test shows that SSL Certificate used on this device is Self-Signed, which is the case in many firewalls that use an https:// management interface. Although this is listed as a medium risk, it is most likely no risk if a Self-Signed SSL Cert is used. To mitigate this medium risk, a Fully Authorized SSL Certificate can be used, however, they can cost upwards of a few hundred dollars or more per year.

22964 (3) - Service Detection – No/Low Risk
This test shows that remote services could be identified. This test simply tries to identify the remote services.

10335 (2) - Nessus TCP scanner - No/Low Risk
It is possible to determine which TCP ports are open (listed on report). If possible turn on filters to prevent access to these open ports from unauthorized addresses.

11219 (2) - Nessus SYN – No/Low Risk
It is possible to determine which TCP ports are open (listed on report). If possible turn on filters to prevent access to these open ports from unauthorized addresses.

10107 (1) - HTTP Server Type and Version – No/Low Risk
This test shows that a web server is running on the ports shown. The 9443 port is a secure https: port commonly used for secure management interfaces. Ensure that access to the management interface of your router is using strong password techniques as described by industry standards. There is no risk factor with this.

10180 (1) - Ping the remote host – No/Low Risk
This test attempts to ping the host using different means to determine if it is up and running. In this case a TCP Syn

packet is used in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK. There is no risk factor with this.

These Ping Statistics show that the host does not respond to a normal ping, which makes the host appear dead (not used) to the public internet using the most common method of discovery. This is a good thing.

10267 (1) - SSH Server Type and Version Information – No/Low Risk
This test attempts to determine that the SSH protocol is running on the port shown. – SSH is a secure Shell program that uses a secure protocol for terminal connections. Ensure that access to the management interface of your router is using strong password techniques as described by industry standards. There is no risk factor with this.

10287 – Traceroute Information (1) – No/Low Risk
This just shows the trace from the testing PC to your network. This information shows the network path through the internet that the testing server takes to gain access to your firewall. It display the addresses of the hops (routers) leading to your internet provider. There is no risk factor with this.

Tracing route to static-10-1-10-11.chi.comcastnet [10.1.10.11]
over a maximum of 30 hops:

For your information, here is the traceroute from 10.1.10.101 to 10.1.10.11 :

10.1.10.101
10.1.10.254
111.245.220.1
81.152.199.98
12.122.132.2
12.123.159.53
12.247.252.26
74.40.2.146
74.42.113.126
10.1.10.11

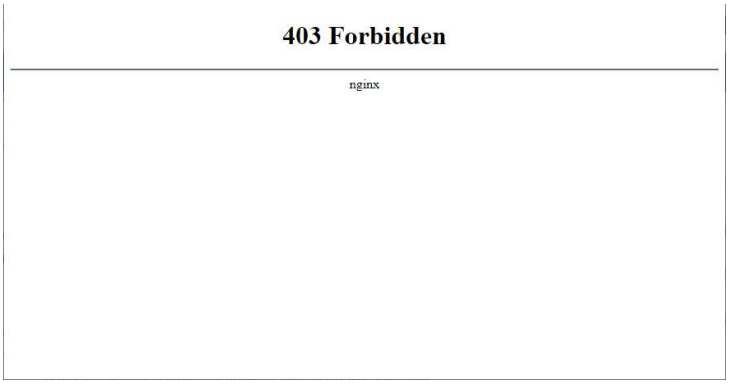
Hop Count: 9
Trace complete.

10662 (1) - Web mirroring – No/Low Risk
The test attempts to make a mirror of the remote website. It shows CGI's that are used on the website. There is no risk factor with this.

10863 (1) - SSL Certificate Information – No/Low Risk
This test connects to every SSL-related port and attempts to extract and dump the X.509 certificate. In this case it is showing the details of the SSL Certificate is a Self-Signed SSL Cert. There is no risk factor with this.

10881 (1) - SSH Protocol Versions Supported – No/Low Risk
This test checks to see if SSH is running on the device. In this case it is. SSH is a secure terminal program used for management purposes of the device. There is no risk factor with this.

11032 (1) - Web Server Directory Enumeration – No/Low Risk
This test checks for possible sub-directories available on the webserver. In this case it found a few that are accessible. However the security of the firewall makes accessing the directories Forbidden. There is no risk factor with this.



11919 (1) - HMAP Web Server Fingerprinting – No/Low Risk
This test attempts to identify the type of web server it is. It is a guess as to what it identifies and states that it could not exactly identify it. There is no risk factor with this.

11935 (1) - IPSEC Internet Key Exchange (IKE) Version 1 Detection – No/Low Risk
This test attempts to determine if a VPN service is running, which it is. There is no risk factor with this.

12053 - Host Fully Qualified Domain Name (FQDN) Resolution – No/Low Risk
This test identifies the DNS of the IP address as: 10.1.10.11resolves as static-184-17-154-235.ftwy.in.frontiernet.net. There is no risk factor with this.

14788 (1) - IP Protocols Scan – No/Low Risk
This test attempts to identify the types of protocols this webserver accepts and understands. It is informational only. There is no risk factor with this.

19506 (1) - Nessus Scan Information – No/Low Risk
This test just displays general information about the Scan that was applied to your device. There is no risk factor with this.

21643 (1) - SSL Cipher Suites Supported – No/Low Risk
This test detects which SSL ciphers are supported by the web server and displays that information. It shows the SSL Encryption types that are used on this host. . It is informational only. There is no risk factor with this.

24260 (1) - HyperText Transfer Protocol (HTTP) Information – No/Low Risk
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... It is informational only. There is no risk factor with this.

25220 (1) - TCP/IP Timestamps Supported – No/Low Risk
This tests determines if the host uses TCP Timestamps, In this case it does. It is informational only. There is no risk factor with this.

43111 (1) - HTTP Methods Allowed (per directory) – No/Low Risk
This plugin determines which HTTP methods are allowed on various CGI directories. It is informational only. There is no risk factor with this

45410 (1) - SSL Certificate 'commonName' Mismatch – No/Low Risk
This test determines the common Name of the SSL Certificate and found the 'commonName' (CN) attribute in the SSL certificate does not match the hostname. This is common on Self-Signed Certificates. There is no risk factor with this

45590 (1) - Common Platform Enumeration (CPE) – No/Low Risk
This test attempts to enumerate CPE (Common Platform Enumeration) names that matched on the remote system. It is a guess but it determined that the system is using OpenBSD and Open SSH on the device. It is informational only. There is no risk factor with this.

49704 (1) - External URLs – No/Low Risk
This test attempts to determine if there are external links on any ot he webpages available on the device. It found Links to external sites for http://www.MyFirewall.com/license/ - /v2/login.php, which is the manufacturer of the device. There is no risk factor with this.

50344 (1) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header – No/Low Risk
This test determines if the web server uses a potential web application vulnerability. By using the Common DNS of the device to access the login page, it shows that CSP frames are not used. However, since this device uses SSL encryption there is no risk factor with this.

50350 (1) - OS Identification Failed – No/Low Risk
This test attempts to determine the OS that the host uses. It could not determine the OS. There is no risk factor with this.

56984 (1) - SSL / TLS Versions Supported – No/Low Risk
This test determines the versions of TLS supported. It found this device supports TLSv1.1/TLSv1.2. There is no risk factor with this.

57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported – No/Low Risk
This test attempts to determine the use of SSL Perfect Forward Secrecy ciphers. In this case it does. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised. There is no risk factor with this.

66334 (1) - Patch Report – No/Low Risk
This test shows the version of the OpenSSH protocol used. It should be upgraded to the latest version. Your firewalls are automatically updated on a regular basis and should be updated on the next round of updates. There is no risk factor with this.

70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported – No/Low Risk
This test attempts to determine the use of SSL Cipher Block Chaining ciphers. In tis case it does. These cipher suites offer additional security over Electronic Codebook (ECB) mode. There is no risk factor with this.

70657 (1) - SSH Algorithms and Languages Supported – No/Low Risk
This test detects which algorithms and languages are supported by the remote service for encrypting communications. There is no risk factor with this.

84502 (1) - HSTS Missing From HTTPS Server – No/Low Risk
This test determines if HTTP Strict Transport Security (HSTS) is used. It is not using this protocol. Which could help prevent some type of attacks. This risk is low to none and is acceptable.

84821 (1) - TLS ALPN Supported Protocol Enumeration – No/Low Risk
This test determines if the TLS ALPN extension is supported. In this case it is. It is informational only. There is no risk factor with this.

91634 (1) - HyperText Transfer Protocol (HTTP) Redirect Information – No/Low Risk
This test determines if an HTTP redirect is used. In this case it does. It is informational only. There is no risk factor with this.

91815 (1) - Web Application Sitemap – No/Low Risk
This test attempts to determine if the remote web server contains linkable content that can be used to gather information about a target. In this case it does. It is informational only. There is no risk factor with this.

94761 (1) - SSL Root Certification Authority Certificate Information
The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. We recommend that you install an updated SSL Certificate for this device. There is no risk factor with this.

110723 (1) - No Credentials Provided – No/Low Risk
This test attempts to determine if common ports are detected. In this case it does for SSH, but there were no credentials provide to log into the device. It is informational only. There is no risk factor with this.

117886 (1) - Local Checks Not Enabled (info) – No/Low Risk
This test attempts to determine if local checks were turned on. They were not and therefore local checks with credentials was not tested. It is informational only. There is no risk factor with this.

121010 (1) - TLS Version 1.1 Protocol Detection – Low Risk
This test determines if TLS 1.1 is supported. In this case it does. It should be deprecated if possible. TLS 1.1 is now

recommend to not be used. The firmware/software on the device should be updated and determined if TLS 1.1 is no longer used. The risk is acceptable at this time.

136318 (1) - TLS Version 1.2 Protocol Detection – Low Risk
This test determines if TLS 1.2 is supported. In this case it does. It should be deprecated if possible. The risk is acceptable at this time.

138614 (1) - Treck/Kasago Network Stack Detection – Low Risk
This test shows that there is a possibility that the device is affected by the Ripple20 vulnerability. Ripple20 is a series of 19 zero-day vulnerabilities found in a widely used, low-level TCP/IP software library developed by Treck, Inc. Ripple20 was disclosed in June, 2020. These vulnerabilities potentially affect hundreds of millions of OT and IoT devices and includes multiple remote code execution (RCE) vulnerabilities. This vulnerability test was developed by JSOF (https://www.jsof-tech.com/). This test attempts to detect the Treck/Kasago network stack on the target system/device via detection alternative methods, also provided by JSOF (https://www.jsof-tech.com/). See website for more info. This test has been known to trigger false positives. We recommend making sure the firewall software is up to date. You may need to contact the firewall vendor for additional information regarding the Treck Vulnerability. See this site for more info on Treck network stack: https://treck.com/vulnerability-response-information/

149334 (1) - SSH Password Authentication Accepted – Low Risk
This test determines if the SSH server on the remote host accepts password authentication. In this case it does. The risk is acceptable at this time.

Other Notes:

There is a web management interface found at ports 9443. It is a secure management interface for your firewall. As shown below:

Make sure that the firewall is password protected using strong password policies as previously described. Access to this server is protected using some form of AES/SSL encryption.

Based on access tests, there appears to be no ftp server, no telnet no SSH server running on normal ports at this IP address. These indicate no external access to this IP address.