Qualys. Express

Scan Results

November 09, 2020

Report Summary	
User Name:	Henry Osei
Login Name:	xc3hs
Company:	X8, LLC.
User Role:	Manager
Address:	1743 Dorsey Road, Suite 112
City:	Hanover
State:	Maryland
Zip:	21076
Country:	United States of America
Created:	11/09/2020 at 08:57:57 (GMT-0500)
Launch Date:	11/08/2020 at 02:04:21 (GMT-0500)
Active Hosts:	1
Total Hosts:	3
Type:	Scheduled
Status:	Finished
Reference:	scan/1604819061.10917
External Scanners:	64.39.99.68 (Scanner 12.1.67-1, Vulnerability Signatures 2.5.27-4)
Duration:	00:09:58
Title:	Firewall Scan
Asset Groups:	-
IPs:	71.244.194.178-71.244.194.180
Excluded IPs:	-
Options Profile:	Continuous Monitoring Scan

Summary of Vulnerabilities

Vulnerabilities Total	7

Security Risk (Avg)	0.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	0	0	0	0
1	0	0	7	7
Total	0	0	7	7

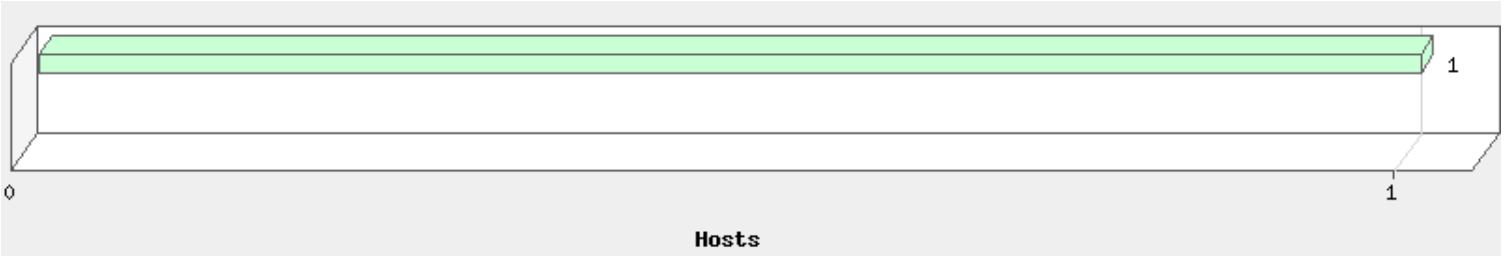
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	5	5
TCP/IP	0	0	1	1
Firewall	0	0	1	1
Total	0	0	7	7

Vulnerabilities by Severity

There are no known vulnerabilities for this/these systems

Operating Systems Detected



Detailed Results

71.244.194.178 (static-71-244-194-178.bltmmd.fios.verizon.net, -)

Information Gathered (7)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
71.244.194.178	static-71-244-194-178.bltmmd.fios.verizon.net

 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-381,383-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1559,1561-1625,1636-1705,
1707-1721,1723-1774,1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,
1973,1981,1985-1999,2001-2028,2030,2032-2033,2035,2038,2040-2049,2053,
2065, and more.
We have omitted from this list 703 higher ports to keep the report size manageable.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The ISP network handle is: NTTA-129-250
ISP Network description:
NTT America, Inc.

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	64.39.99.3	0.29ms	ICMP	
2	216.52.125.61	0.56ms	ICMP	
3	216.52.127.7	1.05ms	ICMP	
4	129.250.200.137	0.54ms	ICMP	
5	129.250.5.215	0.85ms	UDP	80
6	129.250.2.121	0.89ms	ICMP	
7	129.250.8.85	0.72ms	ICMP	
8	100.41.25.9	4.62ms	ICMP	
9	71.244.194.178	6.51ms	ICMP	

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 588 seconds

Start time: Sun, Nov 08 2020, 07:04:31 GMT

End time: Sun, Nov 08 2020, 07:14:19 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
static-71-244-194-178.bltmmd.fios.verizon.net	FQDN

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

Appendix

Hosts Scanned (IP)

71.244.194.178

Target distribution across scanner appliances

External : 71.244.194.178-71.244.194.180

Hosts Not Scanned

Hosts Not Alive (IP) (2)

71.244.194.179-71.244.194.180

Options Profile

Continuous Monitoring Scan

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Kubernetes:	Disabled
Overall Performance:	Normal

Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Enabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	On
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	On
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.