# Audit Report

# Site report for btcnode

Audited on January 22, 2024

Reported on January 22, 2024

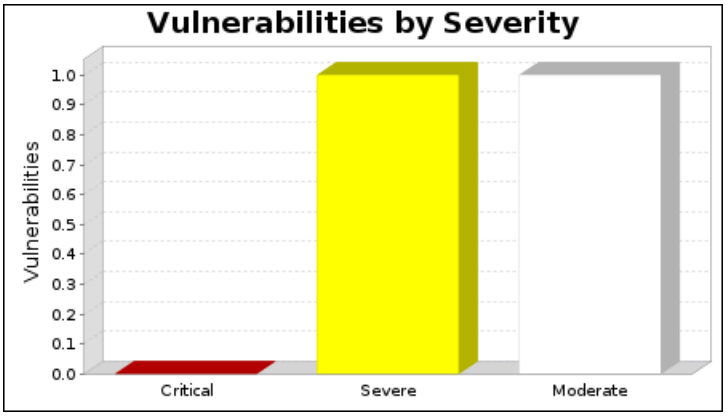
# 1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

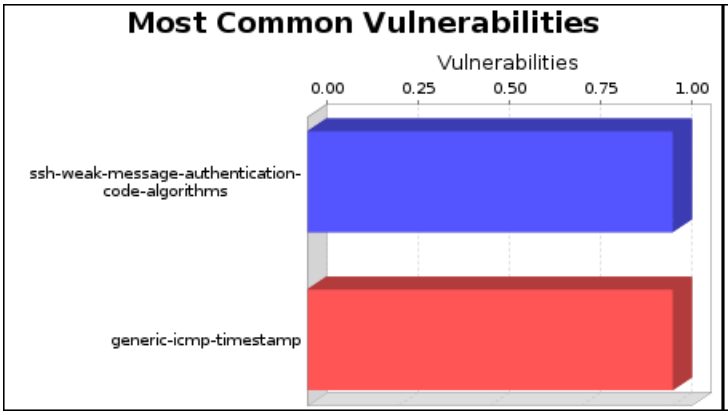
| Site Name | Start Time | End Time | Total Time | Status |
|---|---|---|---|---|
| btcnode | January 22, 2024 15:16, EST | January 22, 2024 15:28, EST | 12 minutes | Success |

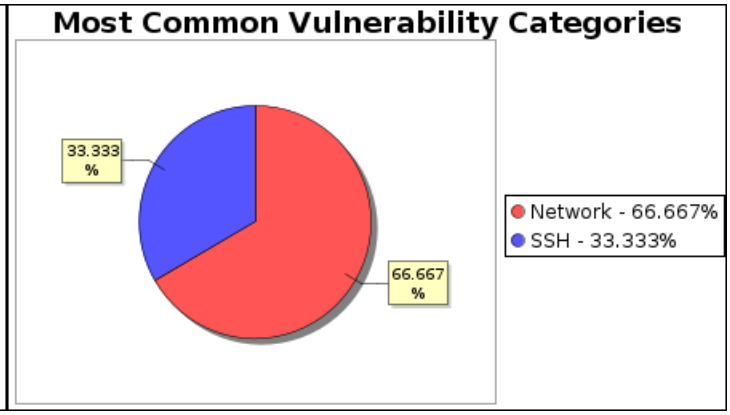
**There is not enough historical data to display risk trend.**

The audit was performed on one system which was found to be active and was scanned.

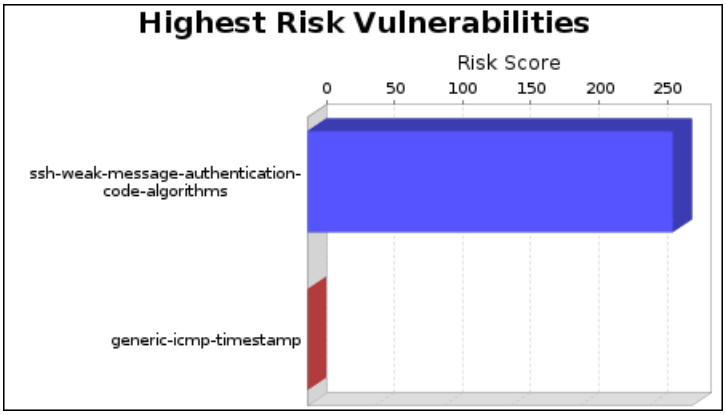



There were 2 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. One vulnerability was severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There was one moderate vulnerability discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

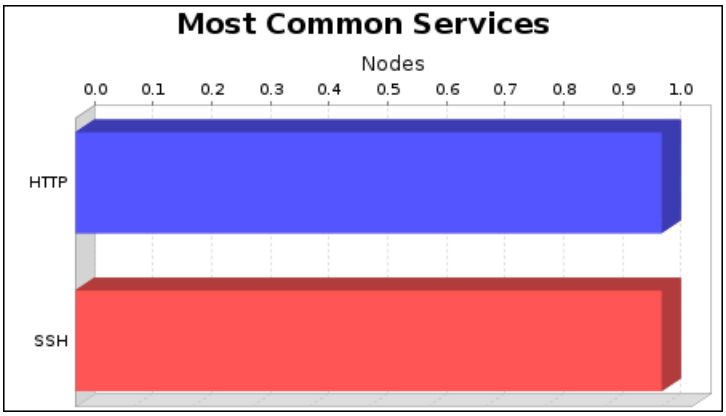



There were 1 occurrences of the ssh-weak-message-authentication-code-algorithms and generic-icmp-timestamp vulnerabilities, making them the most common vulnerabilities. There were 2 vulnerability instances in the Network category, making it the most common vulnerability category.




The ssh-weak-message-authentication-code-algorithms vulnerability poses the highest risk to the organization with a risk score of 268.
Risk scores are based on the types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.
There were 3 services found to be running during this scan.




The HTTP and SSH services were found on 1 systems, making them the most common services.

# 2. Discovered Systems

| Node | Operating System | Risk | Aliases |
|---|---|---|---|
| 192.168.0.103 | Debian Linux 10.0 | 268 | |

# 3. Discovered and Potential Vulnerabilities

## 3.1. Critical Vulnerabilities

No critical vulnerabilities were reported.

## 3.2. Severe Vulnerabilities

### 3.2.1. SSH Weak Message Authentication Code Algorithms (ssh-weak-message-authentication-code-algorithms)

*Description:*

The SSH server supports cryptographically weak Hash-based message authentication codes (HMACs) including MD5 or 96-bit Hash-based algorithms.

*Affected Nodes:*

| Affected Nodes: | Additional Information: |
|---|---|
| 192.168.0.103:22 | Running SSH serviceInsecure MAC algorithms in use: umac-64-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,hmac-sha1 |

*References:*

| Source | Reference |
|---|---|
| URL | https://tools.cisco.com/security/center/resources/next_generation_cryptography |

*Vulnerability Solution:*

Consult the product documentation for instructions to disable any insecure MD5 or 96-bit HMAC algorithms within the SSH configuration.

## 3.3. Moderate Vulnerabilities

### 3.3.1. ICMP timestamp response (generic-icmp-timestamp)

*Description:*

ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

*Affected Nodes:*

| Affected Nodes: | Additional Information: |
|---|---|
| | |

| Affected Nodes: | Additional Information: |
|---|---|
| 192.168.0.103 | Able to determine remote system time. |

*References:*

| Source | Reference |
|---|---|
| CVE | CVE-1999-0524 |
| OSVDB | 95 |
| XF | 306 |
| XF | 322 |

*Vulnerability Solution:*

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

deny icmp any any 13

deny icmp any any 14

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

permit icmp any any unreachable

permit icmp any any echo-reply

permit icmp any any time-exceeded

permit icmp any any source-quench

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

ipchains -A input -p icmp --icmp-type timestamp-request -j DROP

ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

sysctl -w net.inet.icmp.tstamprepl=0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

icmp deny any 13 <inside>

icmp deny any 14 <inside>

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0

/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.

2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

# 4. Discovered Services

## 4.1. <unknown>

### 4.1.1. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 192.168.0.103 | tcp | 8000 | 0 | |

## 4.2. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

### 4.2.1. General Security Issues

*Simple authentication scheme*

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

### 4.2.2. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 192.168.0.103 | tcp | 80 | 0 | •nginx 1.17.8<br>•http.banner: nginx/1.17.8<br>•http.banner.server: nginx/1.17.8 |
| 192.168.0.103 | tcp | 81 | 0 | •http.banner: Express<br>•http.banner.x-powered-by: Express |
| 192.168.0.103 | tcp | 2000 | 0 | •verbs-1: GET<br>•verbs-2: HEAD<br>•verbs-count: 2 |
| 192.168.0.103 | tcp | 2100 | 0 | |
| 192.168.0.103 | tcp | 8080 | 0 | |

## 4.3. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

### 4.3.1. Discovered Instances of this Service

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| 192.168.0.103 | tcp | 22 | 1 | •OpenBSD OpenSSH 7.9p1<br>•ssh.algorithms.compression: none,zlib@openssh.com<br>•ssh.algorithms.encryption: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com<br>•ssh.algorithms.hostkey: rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519<br>•ssh.algorithms.kex: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,kex-strict-s-v00@openssh.com<br>•ssh.algorithms.mac: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1<br>•ssh.banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u4<br>•ssh.hostkey.ecdsa.bits: 256<br>•ssh.hostkey.ecdsa.fingerprint: 81:32:c9:9f:93:16:64:b2:ff:93:25:6e:ab:b4:94:27<br>•ssh.hostkey.ed25519.bits: 256<br>•ssh.hostkey.ed25519.fingerprint: |

| Device | Protocol | Port | Vulnerabilities | Additional Information |
|---|---|---|---|---|
| | | | | ce:7c:41:89:fe:ac:1d:73:c3:41:15:49:c6:6f:2e:af<br>•ssh.hostkey.rsa.bits: 2048<br>•ssh.hostkey.rsa.fingerprint: e9:ca:96:f2:7b:dd:d2:15:1c:75:75:3c:83:3d:67:d6<br>•ssh.hostkey.type: RSA,ECDSA,ED25519<br>•ssh.protocol.version: 2.0 |

# 5. Discovered Users and Groups

No user or group information was discovered during the scan.

# 6. Discovered Databases

No database information was discovered during the scan.

# 7. Discovered Files and Directories

No file or directory information was discovered during the scan.

# 8. Policy Evaluations

No policy evaluations were performed.

# 9. Spidered Web Sites

No web sites were spidered during the scan.