HIPAA Assessment
External Vulnerability Scan Detail Report

Prepared for:

My Client’s Company

Prepared by:

AMS Networks

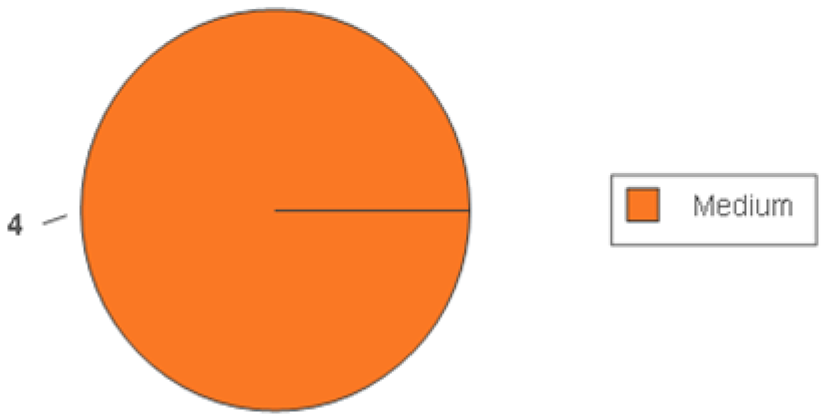
CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 01-Oct-2019

Table of Contents

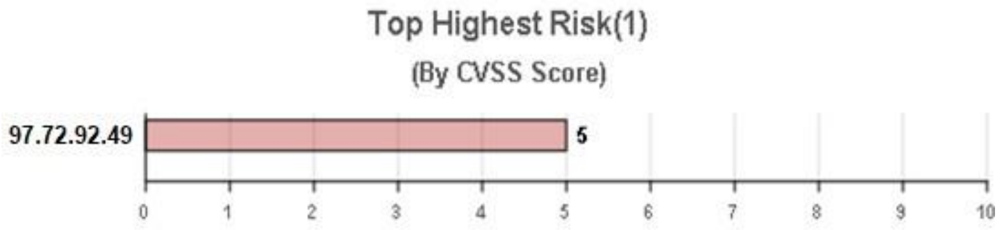
1 - Summary

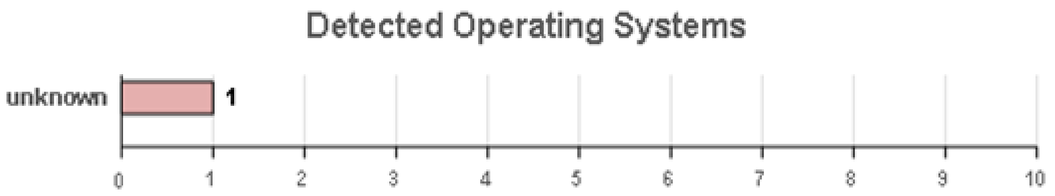
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.

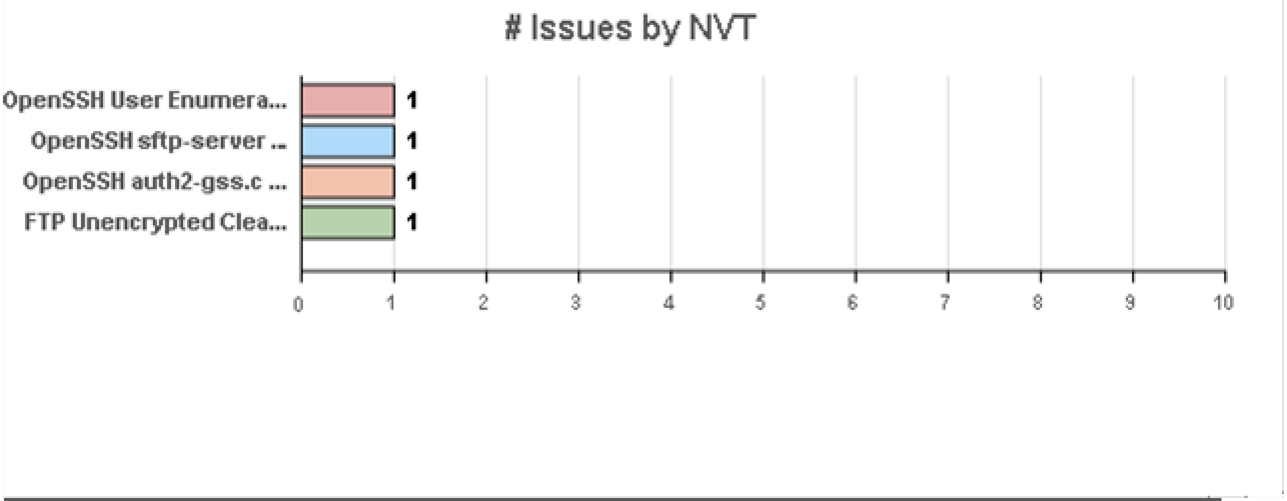


Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
97.72.92.49 (97-72-92-49-static.atl.earthlinkbusiness.net)	4	0	4	0	0	5.0
Total: 1	4	0	4	0	0	5.0

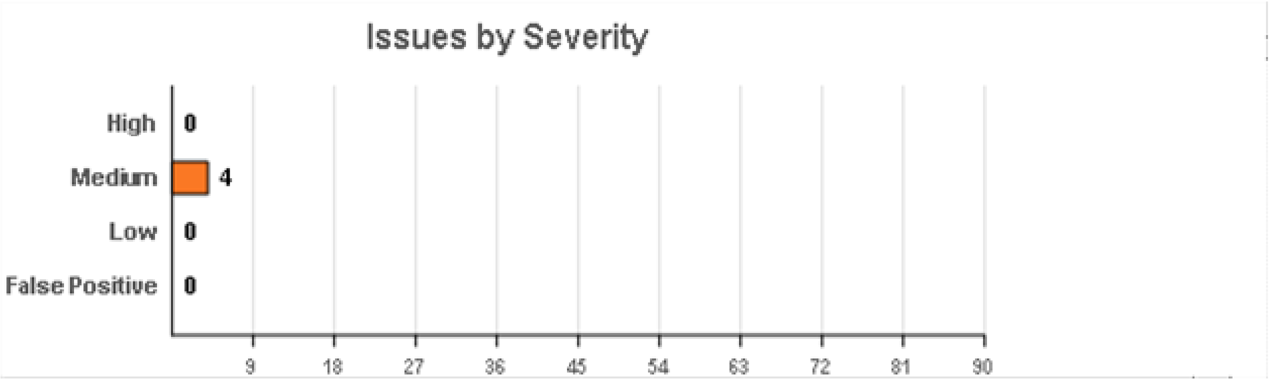




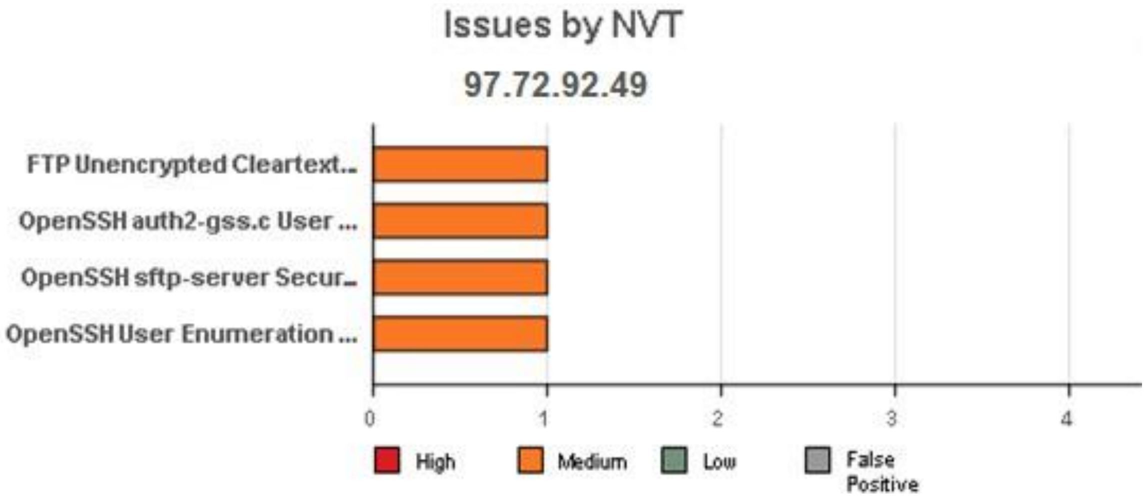


Issue	Count
OpenSSH User Enumeration Vulnerability-Aug18 (Windows)	1
OpenSSH sftp-server Security Bypass Vulnerability (Windows)	1
OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows)	1
FTP Unencrypted Cleartext Login	1

2 - Scan Details



2.1 - 97.72.92.49 (97-72-92-49-static.atl.earthlinkbusiness.net)



Issue	Count
FTP Unencrypted Cleartext Login	1
OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows)	1
OpenSSH sftp-server Security Bypass Vulnerability (Windows)	1
OpenSSH User Enumeration Vulnerability-Aug18 (Windows)	1

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
97.72.92.49 (97-72-92-49-static.atl.earthlinkbusiness.net)	4	0	4	0	0	5.0

Listening Ports

Port
21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 33089/tcp

NVT Issues Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
FTP Unencrypted Cleartext Login	21/tcp (ftp)	**0**	**1**	0	0	4.8
OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows)	22/tcp (ssh)	**0**	**1**	0	0	5.0
OpenSSH sftp-server Security Bypass Vulnerability (Windows)	22/tcp (ssh)	**0**	**1**	0	0	5.0
OpenSSH User Enumeration Vulnerability-Aug18 (Windows)	22/tcp (ssh)	**0**	**1**	0	0	5.0

Security Issues

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)
21/tcp (ftp)

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s): Anonymous sessions: 331 Password required Non-anonymous sessions: 331 Password required

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command. Details: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528) Version used: $Revision: 13611 $

Medium (CVSS: 5)
NVT: OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.813887)
22/tcp (ssh)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.5 Fixed version: None Installation path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
No known solution is available as of 21th May, 2019. Information regarding this issue will be updated once solution details are available.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host. Details: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.813887) Version used: 2019-05-21T12:48:06+0000

References
https://bugzilla.novell.com/show_bug.cgi?id=1106163, https://seclists.org/oss-sec/2018/q3/180

Medium (CVSS: 5)
NVT: OpenSSH sftp-server Security Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.812050)
22/tcp (ssh)

Summary
This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.5 Fixed version: 7.6 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform

unauthorized actions. This may lead to further attacks.

Solution
Upgrade to OpenSSH version 7.6 or later.

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host. Details: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.812050) Version used: 2019-05-21T12:48:06+0000

References
https://www.openssh.com/txt/release-7.6, https://github.com/openbsd/src/commit/a6981567e8e

M **Medium** (CVSS: 5)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Windows)
(OID: 1.3.6.1.4.1.25623.1.0.813863)
22/tcp (ssh)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.5 Fixed version: 7.8 Installation path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Update to version 7.8 or later.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host. Details: OpenSSH User Enumeration Vulnerability-Aug18 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.813863) Version used: 2019-05-21T12:48:06+0000

References
https://0day.city/cve-2018-15473.html,
https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0