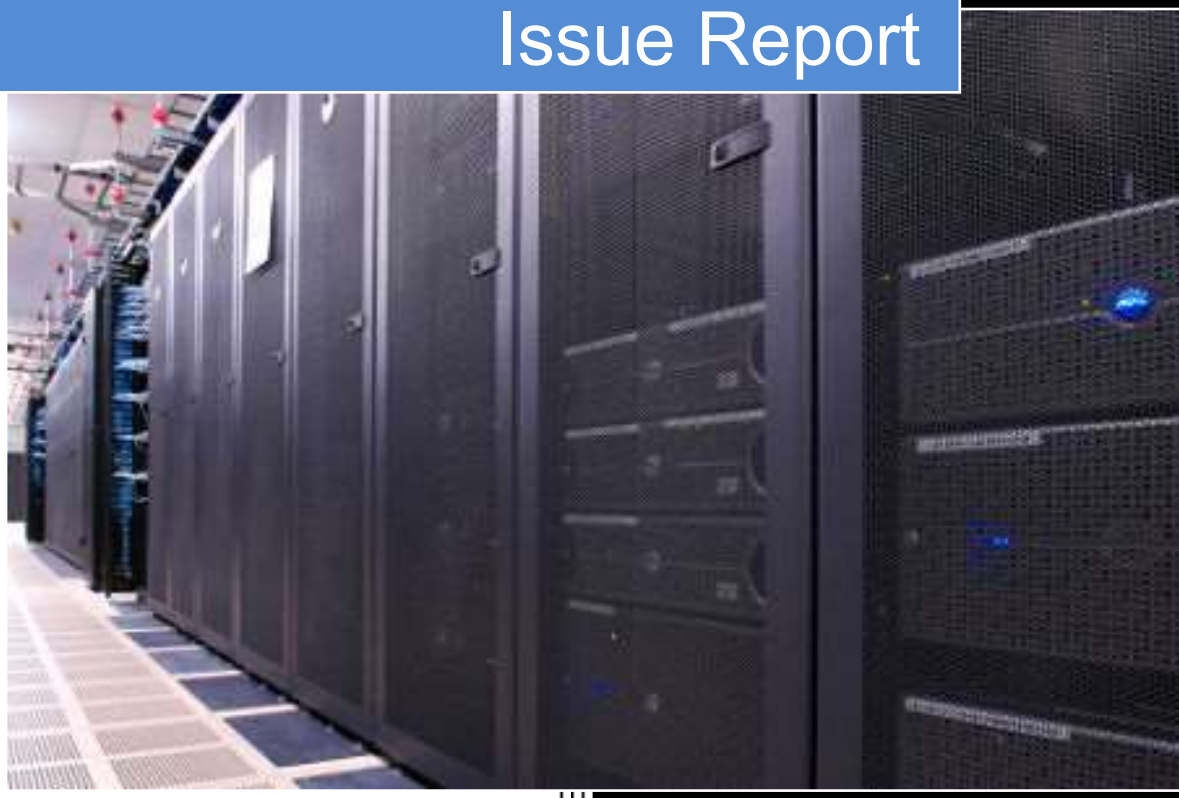
YourIT!
Your Logo Goes Here

NIST CSF Assessment

External Vulnerability Scan Detail by Issue Report

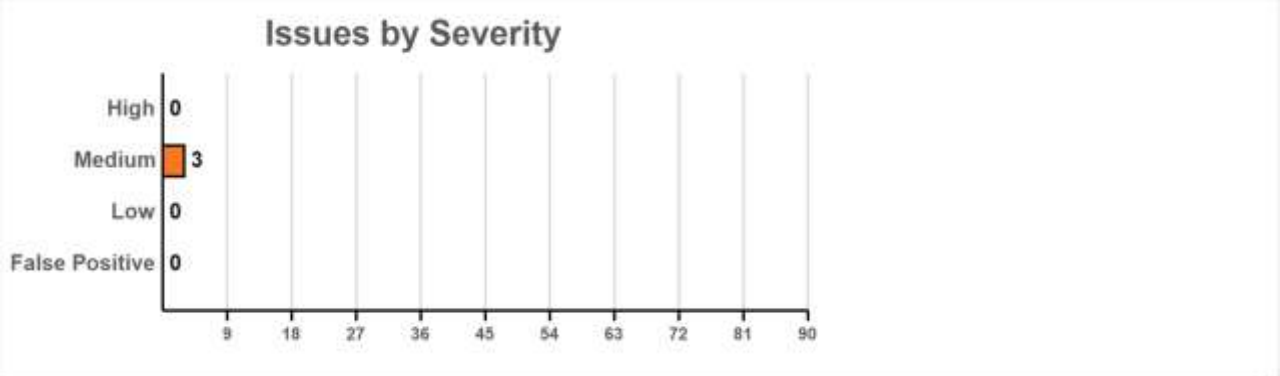


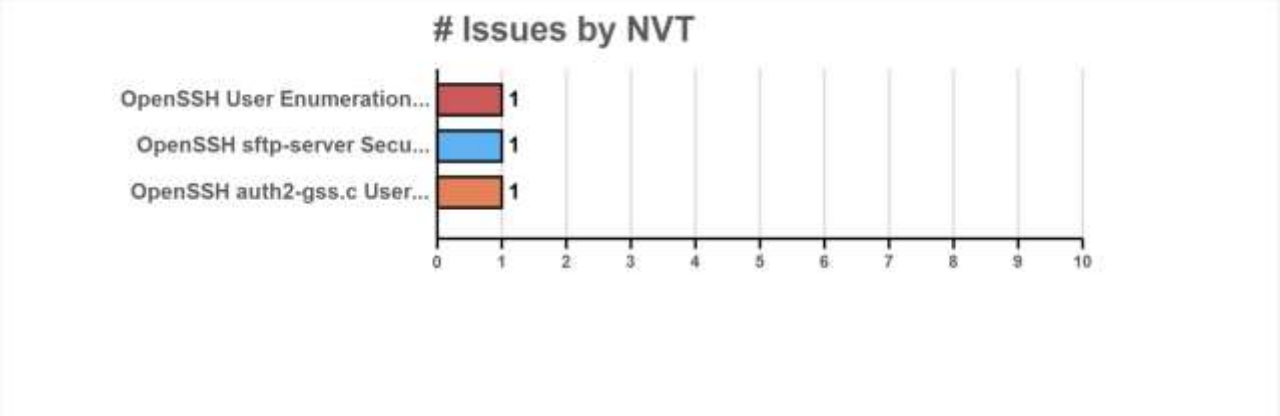
Prepared for:
Your Client's Company
Prepared by:
YourIT Company

Table of Contents

1 - Summary

This report gives details on hosts that were tested and issues that were found during the External Vulnerability Scan. The findings are grouped by category.

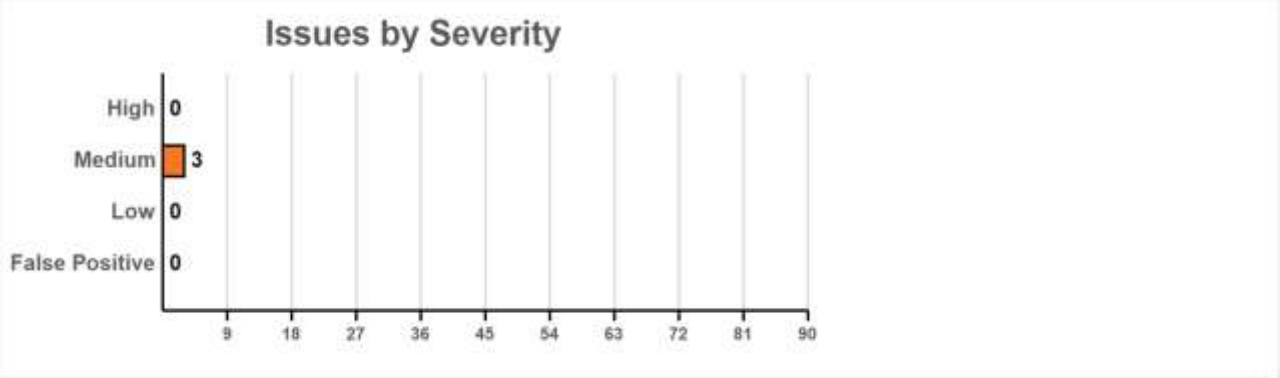




Issue	Count
OpenSSH User Enumeration Vulnerability-Aug18 (Windows)	1
OpenSSH sftp-server Security Bypass Vulnerability (Windows)	1
OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows)	1

2 - Scan Details

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.



2.1 - OpenSSH User Enumeration Vulnerability-Aug18 (Windows)

Medium: (CVSS: 5)
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.

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

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

2.2 - OpenSSH sftp-server Security Bypass Vulnerability (Windows)

Medium: (CVSS: 5)
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.

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

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

2.3 - OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows)

Medium: (CVSS: 5)
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.

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

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 was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

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: 2019-09-26T09:12:46+0000

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