

10.247.2.106

February 18, 2022

Report Summary	
User Name:	Harjeet Singh
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, 1st Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Uttar Pradesh
Zip:	110053
Country:	India
Created:	18 Feb 2022 12:04:29 PM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.2.106
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 18 Feb 2022
Active Hosts:	1
Hosts Matching Filters:	1

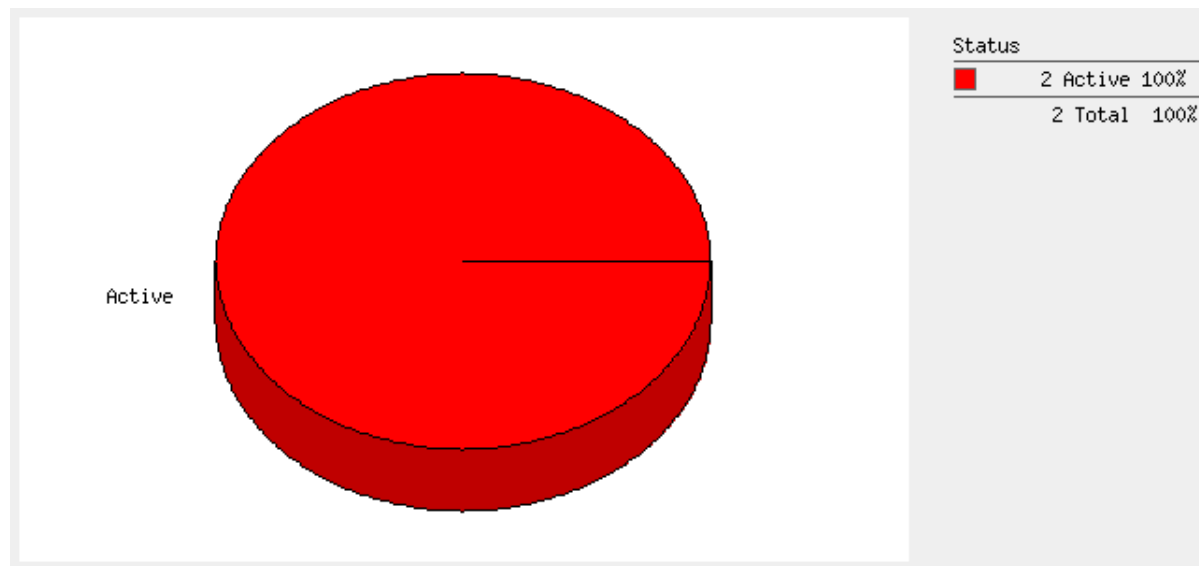
Summary of Vulnerabilities

Vulnerabilities Total	2	Security Risk (Avg)	 3.0	Business Risk	 64/100
-----------------------	---	---------------------	---	---------------	--

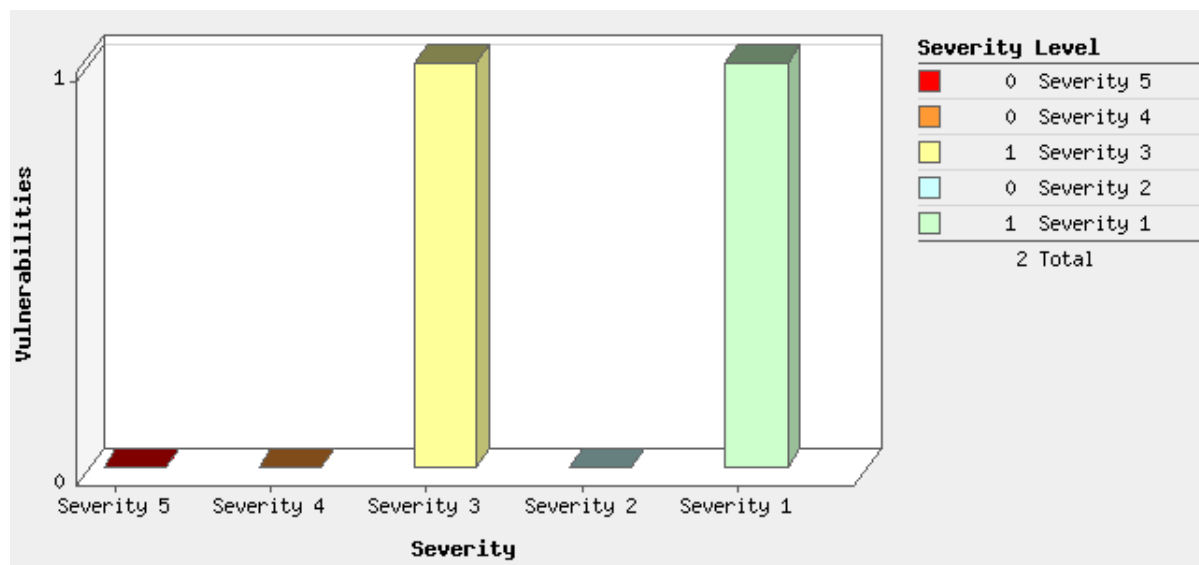
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	1	-	-	1
2	0	-	-	0
1	1	-	-	1
Total	2	-	-	2

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Security Policy	1	-	-	1
Local	1	-	-	1
Total	2	-	-	2

Vulnerabilities by Status

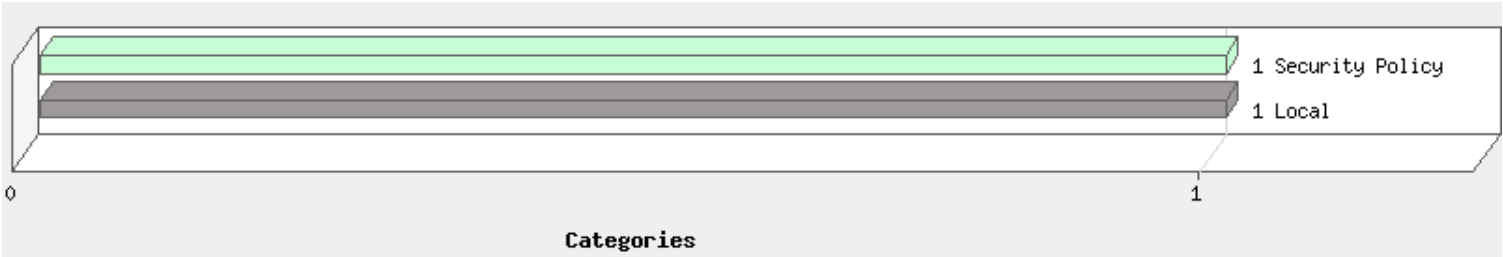


Vulnerabilities by Severity

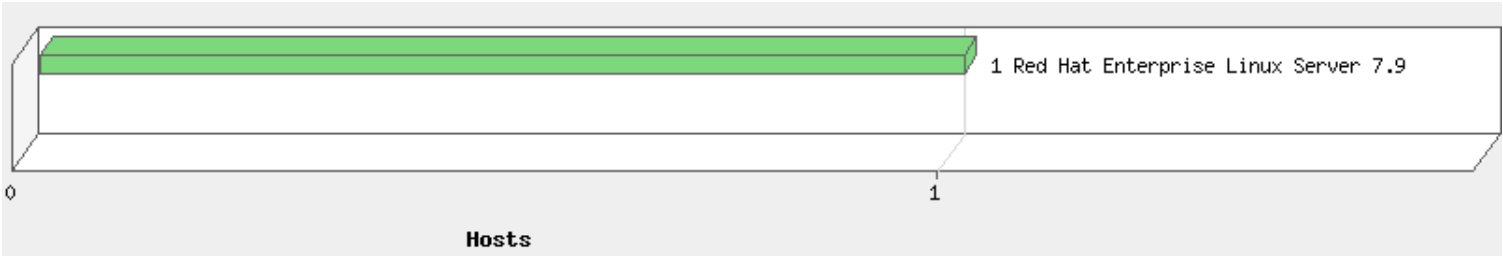


There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.2.106 (sd01p-msdeapp-004.spwh-lxclld.nic.in, -) Red Hat Enterprise Linux Server 7.9

Host Identification Information	
IPs	
QG Host ID	e37806f7-ad78-4065-8f61-c9760da3b542

Vulnerabilities Total	2	Security Risk	<div><div></div><div></div><div></div><div></div><div></div></div>	3.0
-----------------------	---	---------------	--	-----

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

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Security Policy	1	-	-	1
Local	1	-	-	1
Total	2	-	-	2

Vulnerabilities (2)



3 Nmap Buffer Overrun Vulnerability

CVSS: - CVSS3: 6.8 **Active**

QID: 375971
 Category: Local
 CVE ID: [CVE-2021-3712](#)
 Vendor Reference: [Nmap Changelog](#)
 Bugtraq ID: -
 Service Modified: 24 Jan 2022
 User Modified: -
 Edited: No
 PCI Vuln: Yes
 Ticket State:

CVSS Base: 5.8
 CVSS Temporal: 4.9

CVSS3 Base: 7.4
 CVSS3 Temporal: 6.8

First Detected: 17 Jan 2022 10:10:07 PM (GMT+0530)
 Last Detected: 18 Feb 2022 07:34:21 AM (GMT+0530)
 Times Detected: 74
 Last Fixed: N/A

CVSS Environment:

Asset Group: -
 Collateral Damage Potential: -
 Target Distribution: -
 Confidentiality Requirement: -
 Integrity Requirement: -
 Availability Requirement: -

THREAT:

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

The QID checks for vulnerability that exists in the OpenSSL library used by Nmap. It affects latest version of Nmap as it uses OpenSSL 1.1.1k. The Vulnerability has been fixed in OpenSSL 1.1.1l and may be fixed in the future Nmap release.

Affected Software:
Nmap upto version 7.92.

QID Detection Logic (Authenticated Unix):

This QID checks for vulnerable versions of nmap by executing "nmap --version" command.

QID Detection Logic (Authenticated Windows) :

This QID checks for vulnerable versions of nmap using file "nmap.exe" version.

NOTE: The Windows check will only work for nmap when downloaded nmap using self-installer.

IMPACT:

Successful exploitation could allow attacker to read buffer overruns processing ASN.1 strings.

SOLUTION:

Currently no patch is available to fix this vulnerability but users are advised to install latest version of nmap from nmap download page

(<http://nmap.org/download.html>).

RESULTS:

Vulnerable Nmap version is detected.

Nmap version 6.40 (<http://nmap.org>)



1 World-Writable Directories Should Have Their Sticky Bits Set

CVSS: - CVSS3: - **Active**

QID: 105146
Category: Security Policy
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 18 Mar 2021
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

CVSS Base: 0 [\[1\]](#)
CVSS Temporal: 0

CVSS3 Base: -
CVSS3 Temporal: -

First Detected: 17 Jan 2022 10:10:07 PM (GMT+0530)

Last Detected: 18 Feb 2022 07:34:21 AM (GMT+0530)

Times Detected: 74

Last Fixed: N/A

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

The Results section lists world-writable directories whose sticky bits are not set.

IMPACT:

N/A

SOLUTION:

It's best practice to set the sticky bit for world-writable directories.

RESULTS:

/tmp/
/var/tmp/

Appendix






Report Filters

Excluded Vulnerability Lists:	OpenSSH Information Disclosure Vulnerability (Generic) _CVE-2020-14145
Excluded QIDs:	650035
Status:	New, Active, Re-Opened
Display non-running kernels:	Off
Exclude non-running kernels:	On
Exclude non-running services:	Off
Exclude QIDs not exploitable due to configuration:	Off
Vulnerabilities:	State:Active
Included Operating Systems:	All Operating Systems

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.

Severity	Level	Description
 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.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.

CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2022, Qualys, Inc.