Qualys. Cloud Platform

National Informatics Centre

10.247.202.209

July 27, 2023

Report Summary	
User Name:	Rahul Tyagi
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, Ist Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Delhi
Zip:	110053
Country:	India
Created:	27 Jul 2023 09:44:11 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.202.209
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 27 Jul 2023
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	1	Security Risk (Avg)	4.0	Business Risk	36/100

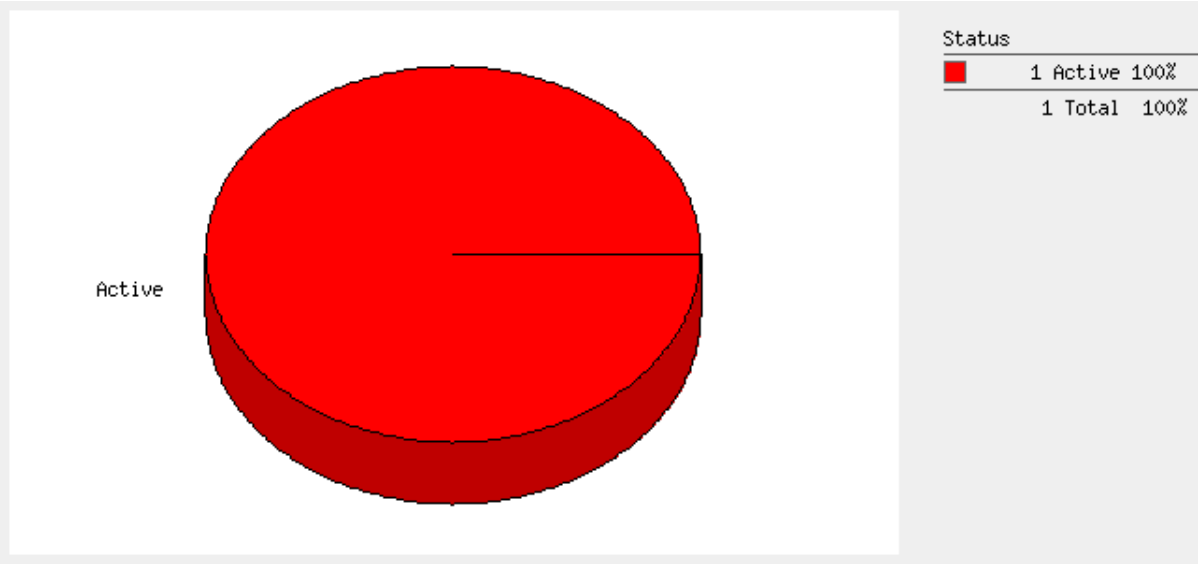
by Severity

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

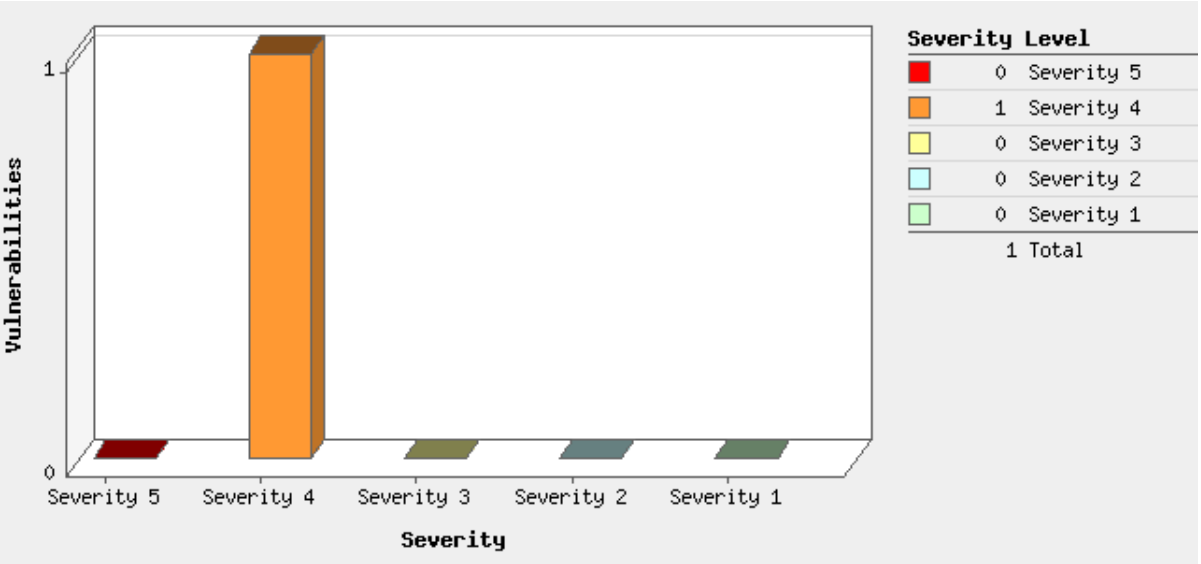
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Local	1	-	-	1
Total	1	-	-	1

Vulnerabilities by Status



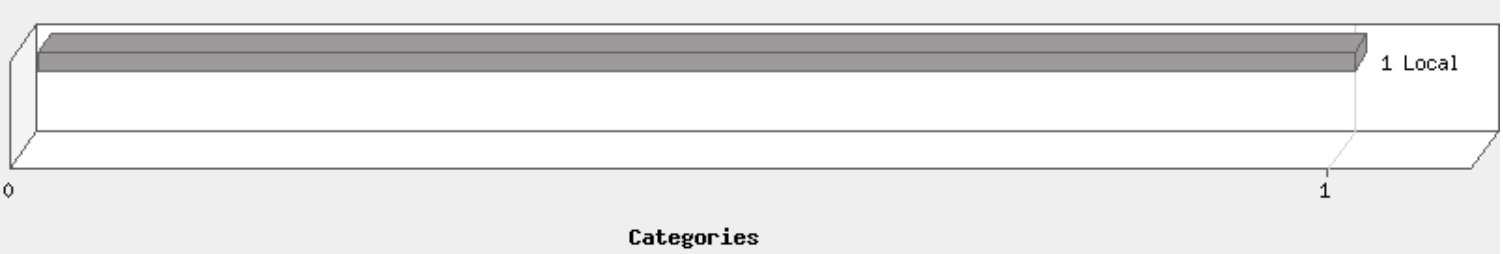
Vulnerabilities by Severity



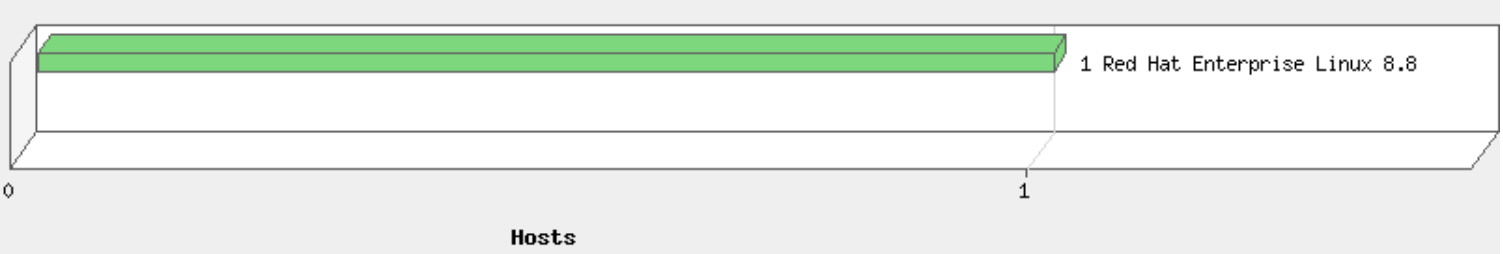
Information Gathered by Severity

There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.202.209 (to03p-iiwapsr-001.webcloud3.nic.in, -) Red Hat Enterprise Linux 8.8

Host Identification Information	
IPs	
QG Host ID	bcc77e6d-6f14-419f-9db5-6daa6970ea68

Vulnerabilities Total	1	Security Risk	4.0

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

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

Vulnerabilities (1)

4 Oracle Java Standard Edition (SE) Critical Patch Update - July 2023 (CPUJUL2023) CVSS: 6.9 CVSS3.1: 6.5 Active

QID:	378673	CVSS Base:	9.3 [1]
Category:	Local	CVSS Temporal:	6.9
Associated CVEs:	CVE-2023-22043, CVE-2023-22041, CVE-2023-25193, CVE-2023-22044, CVE-2023-22045, CVE-2023-22049, CVE-2023-22036, CVE-2023-22006		
Vendor Reference:	Oracle Critical Patch Update Advisory - July 2023		
Bugtraq ID:	-		
Service Modified:	20 Jul 2023	CVSS3.1 Base:	7.5
User Modified:	-	CVSS3.1 Temporal:	6.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:	Open		

First Detected: 21 Jul 2023 03:39:24 PM (GMT+0530)

Last Detected: 27 Jul 2023 06:03:32 AM (GMT+0530)

Times Detected: 16

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Oracle Java Runtime Environment (JRE) is a platform that supports the execution of programs that are developed using the Java programming language. The JRE platform also supports Java Applets, which can be loaded from Web pages.
Oracle Java JRE and JDK contain multiple remotely exploitable vulnerabilities that affect various components.
Affected Versions:
Oracle Java SE : Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1 and prior
QID Detection Logic (Authenticated):
Operating System: Windows
This QID checks for the file or product version of jvm.dll or wsdetect.dll or verify.dll.
QID Detection Logic (Authenticated):
Operating System: Linux
This QID checks product version from the java binary.

IMPACT:

Successful exploitation could allow an attacker to affect the confidentiality, and integrity of data, obtain elevated privileges or could cause high data loss on the target system.

SOLUTION:

The vendor has released updates to resolve these issues.
Customers are advised to refer to vendor advisory Oracle Critical Patch Update Advisory - July2023 (https://www.oracle.com/security-alerts/cpujul2023.html#AppendixJAVA)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Oracle Critical Patch Update Advisory - July 2023 (https://www.oracle.com/security-alerts/cpujul2023.html)

RESULTS:

Install Location	Version	Detection Type
/usr/lib/jvm/jdk-11-oracle-x64/bin/java	11.0.19+9-LTS-224	Default

Appendix

Report Filters

Excluded Vulnerability Lists:	Exclusion RHEL Mariadb (QID- 240255), OpenSSH Information Disclosure Vulnerability (Generic) _CVE-2020-14145
Excluded QIDs:	240255, 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.