

10.246.115.66

June 07, 2023

Report Summary

User Name:	Rahul Tyagi
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, 1st Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Delhi
Zip:	110053
Country:	India
Created:	07 Jun 2023 08:57:21 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.246.115.66
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 07 Jun 2023
Active Hosts:	1
Hosts Matching Filters:	1

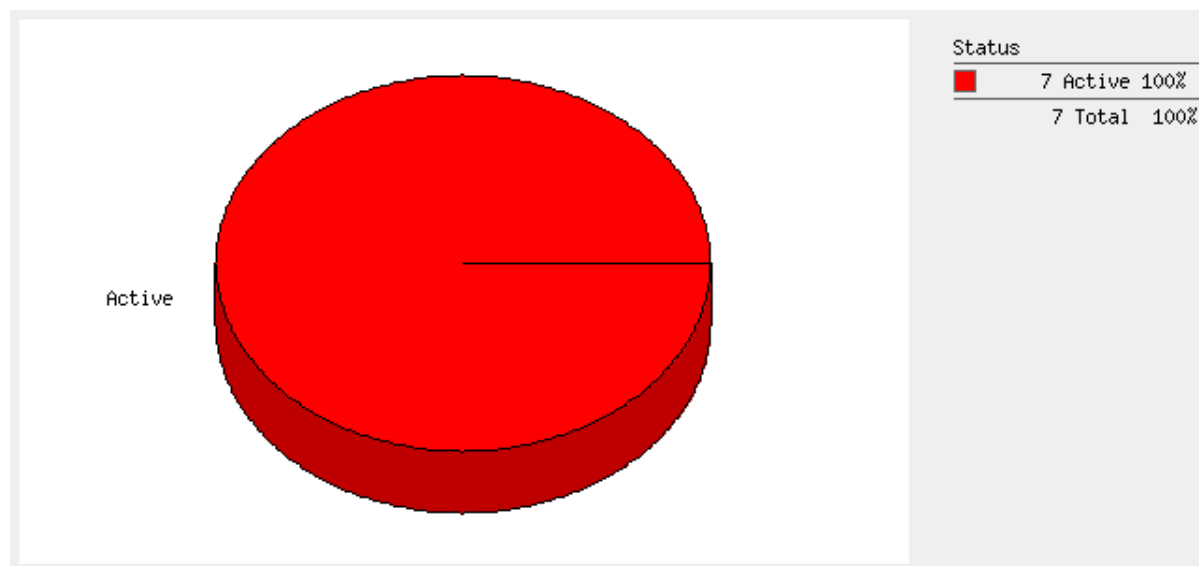
Summary of Vulnerabilities

Vulnerabilities Total	7	Security Risk (Avg)	 5.0	Business Risk	 16/100
-----------------------	---	---------------------	---	---------------	--

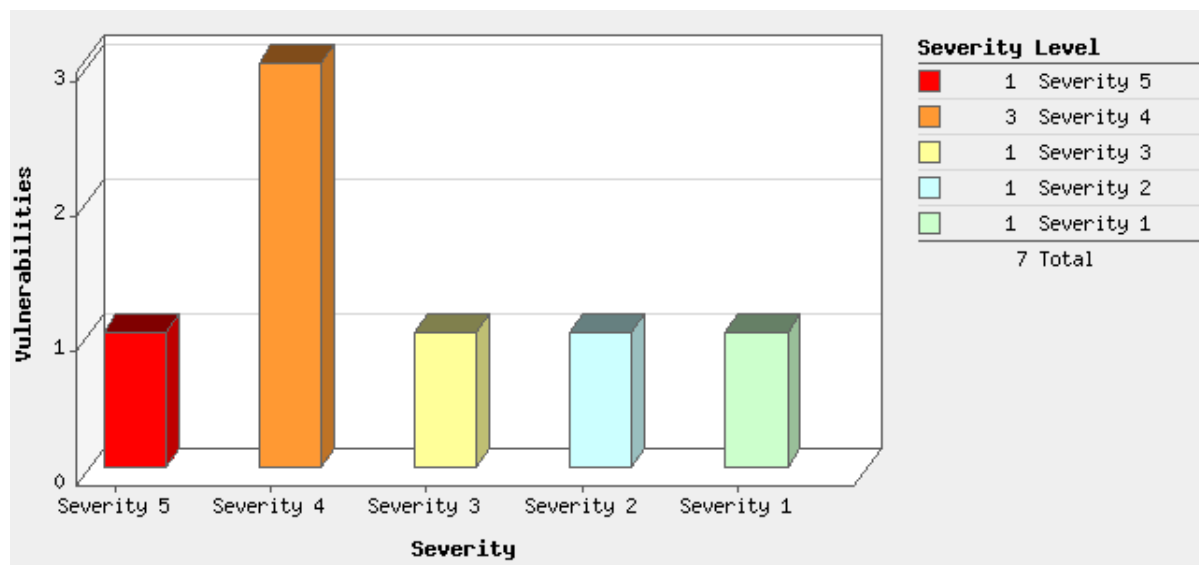
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	-	-	1
4	3	-	-	3
3	1	-	-	1
2	1	-	-	1
1	1	-	-	1
Total	7	-	-	7

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Local	5	-	-	5
Security Policy	2	-	-	2
Total	7	-	-	7

Vulnerabilities by Status

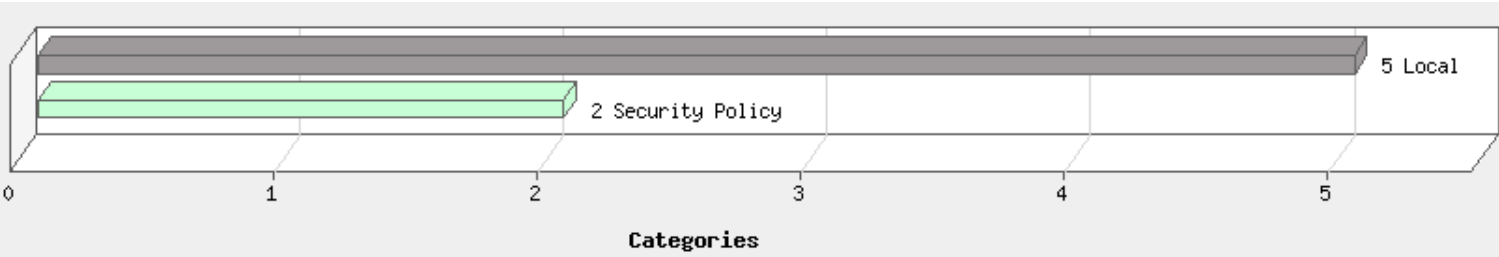


Vulnerabilities by Severity

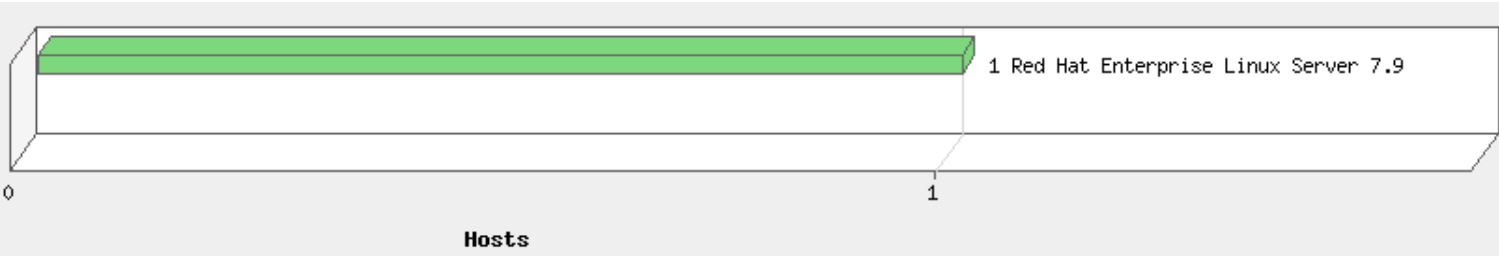


There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.246.115.66 (ea03p-eccssdb-001.webcloud3.nic.in, -) Red Hat Enterprise Linux Server 7.9

Host Identification Information	
IPs	
QG Host ID	a5187326-f888-48e4-b329-e1e7f4cca577

Vulnerabilities Total

7

Security Risk

5.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	-	-	1
4	3	-	-	3
3	1	-	-	1
2	1	-	-	1
1	1	-	-	1
Total	7	-	-	7

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Local	5	-	-	5
Security Policy	2	-	-	2
Total	7	-	-	7

Vulnerabilities (7)


5 EOL/Obsolete Software: Oracle/Sun Java Development Kit (JDK) Java Runtime Environment (JRE) 5 (1.5.x) Detected CVSS: 7.9 CVSS3.1: - **Active**

QID:	105413	CVSS Base:	9.3 [1]
Category:	Security Policy	CVSS Temporal:	7.9
Associated CVEs:	-		
Vendor Reference:	J2SE 5.0 End of Life		
Bugtraq ID:	-		
Service Modified:	01 Mar 2023	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		
Ticket State:	Open		

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)

Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)

Times Detected: 177

Last Fixed: N/A

CVSS Environment:

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

THREAT:

Oracle/Sun Java Runtime Environment 1.5.x was detected on the target host. Support for J2SE 1.5 ended on October 2009 and no further support is available without a support contract.

IMPACT:

The system is at high risk of exposure to security vulnerabilities and obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:

Upgrade to the latest free release available at Java Download site (<http://www.oracle.com/technetwork/java/javase/downloads/index.html>).

RESULTS:

Install Location	Version	Detection Type
/home/oracle/ora_home/jdk/bin/java	1.5.0_51-b10	Enhanced
/home/oracle/ora_home/jdk/jre/bin/java	1.5.0_51-b10	Enhanced



4 Oracle Java SE Critical Patch Update - April 2015

CVSS: 7.8 CVSS3.1: - Active

QID: 123519 CVSS Base: 10.0
Category: Local CVSS Temporal: 7.8
Associated CVEs: [CVE-2015-0469](#), [CVE-2015-0459](#), [CVE-2015-0491](#), [CVE-2015-0460](#), [CVE-2015-0492](#), [CVE-2015-0458](#),
[CVE-2015-0484](#), [CVE-2015-0480](#), [CVE-2015-0486](#), [CVE-2015-0488](#), [CVE-2015-0477](#), [CVE-2015-0470](#),
[CVE-2015-0478](#), [CVE-2015-0204](#)
Vendor Reference: [Oracle Java SE CPU April 2015](#)
Bugtraq ID: [74097](#), [74072](#), [74147](#), [74141](#), [74083](#), [74104](#), [91787](#), [74145](#), [74135](#), [71936](#), [74111](#), [74094](#), [74149](#), [74129](#),
[74119](#)
Service Modified: 29 May 2023 CVSS3.1 Base: -
User Modified: - CVSS3.1 Temporal: -
Edited: No
PCI Vuln: Yes
Ticket State: Open

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)

Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)

Times Detected: 177

Last Fixed: N/A

CVSS Environment:

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

THREAT:

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.

JRE and JDK are exposed to multiple vulnerabilities that affect various components. Oracle's Java Critical Patch Update for April 2015 contains 15 new security fixes across multiple Java SE products and sub-products.

Affected Versions:

Oracle Java JDK and JRE, versions 5.0u81 and earlier, 6u91 and earlier, 7u76 and earlier, 8u40 and earlier.

IMPACT:

Exploitation could allow an attacker to take complete control of an affected system.

SOLUTION:

The vendor released updates (Java SE JDK and JRE 8 Update 45, Java SE JDK and JRE 7 Update 79, Java SE JDK and JRE 6 Update 95, Java SE JDK and JRE 5.0 Update 85) to resolve these issues.

Refer to vendor advisory Oracle Java SE CPU April 2015 (<http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html>) and Oracle Doc ID 1992462.1 (<https://support.oracle.com/rs?type=doc&id=1992462.1>) to obtain more details.

Updates for Java 5 and Java 6 are no longer available to the public. Oracle offers updates to Java 5 and Java 6 only for customers who have purchased Java support or have Oracle products that require Java 5 and Java 6.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Oracle Java SE CPU April 2015: Oracle Java (<http://www.oracle.com/technetwork/java/javase/downloads/index.html>)

RESULTS:

Install Location	Version	Detection Type
/home/oracle/ora_home/jdk/bin/java	1.5.0_51-b10	Enhanced
/home/oracle/ora_home/jdk/jre/bin/java	1.5.0_51-b10	Enhanced



4 Oracle Java Standard Edition (SE) Critical Patch Update - April 2023 (CPUAPR2023)

CVSS: 5.3 CVSS3.1: 6.4 Active

QID: 378425 CVSS Base: 7.1 [1]
Category: Local CVSS Temporal: 5.3
Associated CVEs: [CVE-2023-21930](#), [CVE-2023-21967](#), [CVE-2023-21954](#), [CVE-2023-21939](#), [CVE-2023-21938](#),
[CVE-2023-21968](#), [CVE-2023-21937](#)
Vendor Reference: [Oracle Critical Patch Update Advisory - April 2023](#)
Bugtraq ID: -

Service Modified: 19 Apr 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS3.1 Base: 7.4
CVSS3.1 Temporal: 6.4

First Detected: 20 Apr 2023 09:50:28 AM (GMT+0530)
Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)
Times Detected: 149
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: 8u371, 8u371-perf, 11.0.18, 17.0.6, 20;
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 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 - April 2023 (<https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Oracle Critical Patch Update Advisory - April 2023 (<https://www.oracle.com/security-alerts/cpuapr2023.html>)

RESULTS:

Install Location	Version	Detection Type
/opt/jdk1.8.0_131/jre/bin/java	1.8.0_131-b11	Enhanced
/opt/jdk1.8.0_131/bin/java	1.8.0_131-b11	Enhanced
/usr/opencv/java/jre/bin/java	1.8.0_161-b12	Enhanced

4 McAfee Agent Multiple Vulnerabilities (SB10378)

CVSS: 6.9 CVSS3.1: 6.8 **Active**

QID: 376433
Category: Local
Associated CVEs: [CVE-2021-31854](#), [CVE-2022-0166](#)
Vendor Reference: [SB10378](#)
Bugtraq ID: -
Service Modified: 12 Jan 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State: Open

CVSS Base: 9.3
CVSS Temporal: 6.9

CVSS3.1 Base: 7.8
CVSS3.1 Temporal: 6.8

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)
Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)
Times Detected: 177
Last Fixed: N/A

CVSS Environment:

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

THREAT:

The McAfee Agent is the distributed component of McAfee ePolicy Orchestrator. It downloads and enforces policies, and executes client-side tasks such as deployment and updating. The Agent also uploads events and provides additional data regarding each system status.
McAfee Agent is affected with the following vulnerability:
CVE-2021-31854: A command Injection Vulnerability in McAfee Agent (MA) for Windows prior to 5.7.5 allows local users to inject arbitrary shell code into the file
CVE-2022-0166: A privilege escalation vulnerability in the McAfee Agent prior to 5.7.5 affecting all supported operating systems..

Affected versions:
McAfee Agent Prior to 5.7.5

QID Detection Logic(Authenticated):

The QID checks for vulnerable version of McAfee Agent by checking the version information at HKLM\SOFTWARE\McAfee\Agent registry key for 32/64 bit and /opt/McAfee/agent/bin/msaconfig in Linux to detect the version.

IMPACT:


Successful exploitation of this vulnerability may result command injection and privilege escalation.

SOLUTION:

Install or update to McAfee Agent 5.7.5 For more details refer
SB10378 (<https://kc.mcafee.com/corporate/index?page=content&id=SB10378>)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
SB10378 (<https://kc.mcafee.com/corporate/index?page=content&id=SB10378>)

RESULTS:

```
config=$(cat /opt/McAfee/agent/bin/msaconfig | egrep -o 'etc.*config.xml'); cat "$config" | grep -i '<version>'<br><Version>5.6.1.157</Version>
```

 3 McAfee Agent Multiple Insecure Storage Vulnerability (SB10382)		CVSS: 1.6	CVSS3.1: 4.8	Active
QID:	376619	CVSS Base:	2.1	
Category:	Local	CVSS Temporal:	1.6	
Associated CVEs:	CVE-2022-1257			
Vendor Reference:	SB10382			
Bugtraq ID:	-			
Service Modified:	12 May 2023	CVSS3.1 Base:	5.5	
User Modified:	-	CVSS3.1 Temporal:	4.8	
Edited:	No			
PCI Vuln:	Yes			
Ticket State:				

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)
Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)
Times Detected: 177
Last Fixed: N/A

CVSS Environment:

Asset Group: -

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

THREAT:

The McAfee Agent is the distributed component of McAfee ePolicy Orchestrator. It downloads and enforces policies, and executes client-side tasks such as deployment and updating. The Agent also uploads events and provides additional data regarding each system status.

CVE-2022-1257: Insecure storage of sensitive information vulnerability in MA for Linux, macOS, and Windows prior to 5.7.6 allows a local user to gain access to sensitive information through storage in ma.db.

Affected versions:

McAfee Agent Prior to 5.7.6

QID Detection Logic(Authenticated):

The QID checks for vulnerable version of McAfee Agent by checking the version information at HKLM\SOFTWARE\McAfee\Agent registry key for 32/64 bit and /opt/McAfee/agent/bin/msaconfig in Linux to detect the version.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to steal sensitive information from the target.

SOLUTION:

Install or update to McAfee Agent 5.7.6 For more details refer

SB10382 (<https://kc.mcafee.com/corporate/index?page=content&id=SB10382>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

SB10382 (<https://kc.mcafee.com/corporate/index?page=content&id=SB10382>)

RESULTS:

```
config=$(cat /opt/McAfee/agent/bin/msaconfig | egrep -o 'etc.*config.xml'); cat "$config" | grep -i '<version>'<br><Version>5.6.1.157</Version>
```

 2  Oracle Java Standard Edition (SE) Critical Patch Update - April 2022 (CPUAPR2022) CVSS: 3.9 CVSS3.1: 6.7 Active

QID:	376546	CVSS Base:	5.0
Category:	Local	CVSS Temporal:	3.9
Associated CVEs:	CVE-2022-0778 , CVE-2022-21476 , CVE-2022-21426 , CVE-2022-21496 , CVE-2022-21434 , CVE-2022-21443		
Vendor Reference:	Oracle Critical Patch Update Advisory - April 2022		
Bugtraq ID:	-		
Service Modified:	01 Jun 2023	CVSS3.1 Base:	7.5
User Modified:	25 Jun 2022	CVSS3.1 Temporal:	6.7
Edited:	Yes		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)

Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)

Times Detected: 177

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 JDK and JRE, versions 7u331, 8u321, 11.0.14, 17.0.2, 18 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, integrity and availability of data 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 - April 2022 (<https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixJAVA>)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Oracle Critical Patch Update Advisory - April 2022 (<https://www.oracle.com/security-alerts/cpuapr2022.html>)

SOLUTION COMMENTS:

Mail received By Avtar Sir, on 25June2022,SR#103357

RESULTS:

Install Location	Version	Detection Type
/opt/jdk1.8.0_131/jre/bin/java	1.8.0_131-b11	Enhanced
/opt/jdk1.8.0_131/bin/java	1.8.0_131-b11	Enhanced
/usr/opencv/java/jre/bin/java	1.8.0_161-b12	Enhanced



1 World-Writable Directories Should Have Their Sticky Bits Set

CVSS: 0 CVSS3.1: - Active

QID: 105146
Category: Security Policy
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12 May 2023
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

CVSS Base: 0.0 [1]
CVSS Temporal: 0.0

CVSS3.1 Base: -
CVSS3.1 Temporal: -

First Detected: 11 Apr 2023 04:08:13 PM (GMT+0530)

Last Detected: 07 Jun 2023 05:03:19 AM (GMT+0530)

Times Detected: 177

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:

/usr/netvault/tmp

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.

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 2023, Qualys, Inc.