Qualys. Cloud Platform

National Informatics Centre

10.247.187.200

May 29, 2023

Report Summary	
User Name:	Harjeet Singh
Company:	NIC -NDCSP
User Role:	Manager
Address:	BLOCK 3, Ist Floor NDC, Delhi IT Park Shastri Park
City:	New Delhi
State:	Uttar Pradesh
Zip:	110053
Country:	India
Created:	29 May 2023 09:18:11 AM (GMT+0530)
Template Title:	NIC report template
Asset Groups:	-
IPs:	10.247.187.200
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01 Jan 1999 - 29 May 2023
Active Hosts:	1
Hosts Matching Filters:	1

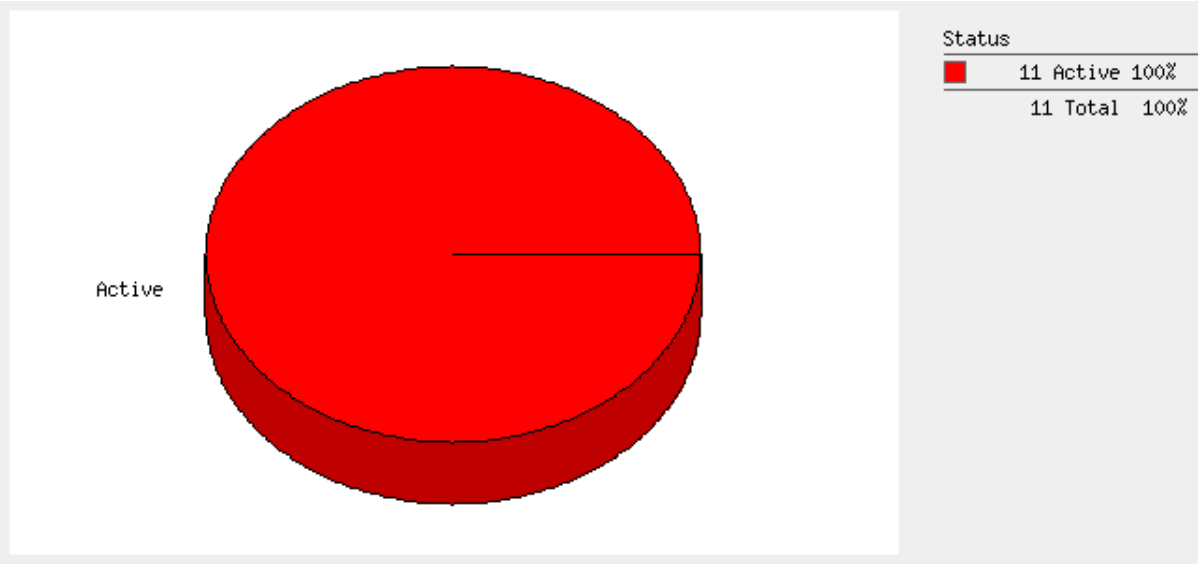
Summary of Vulnerabilities

Vulnerabilities Total	11	Security Risk (Avg)	5.0	Business Risk	16/100

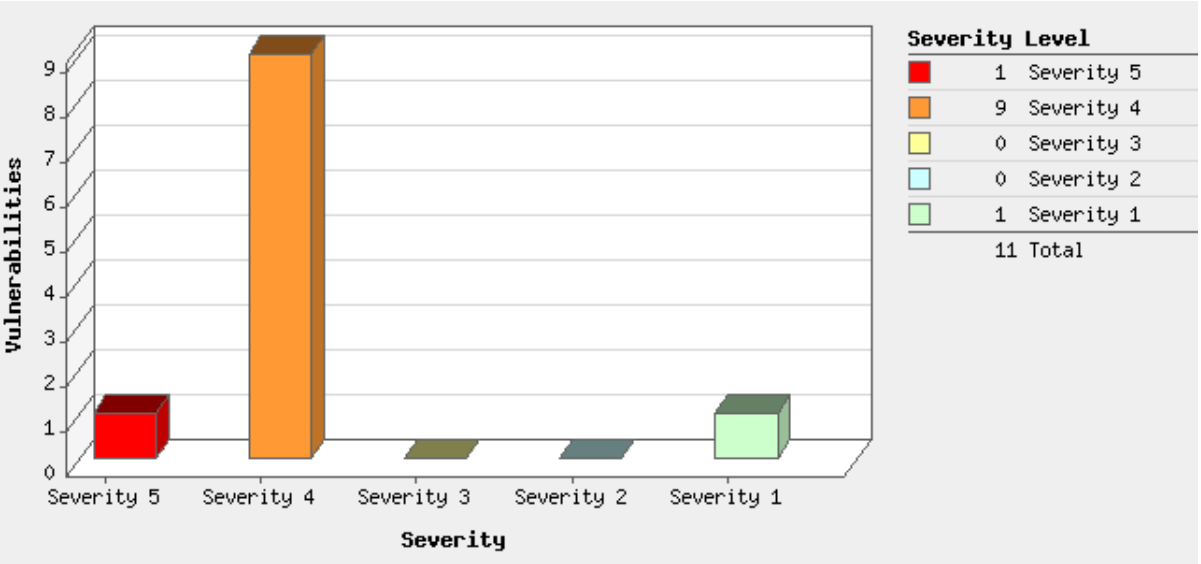
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	-	-	1
4	9	-	-	9
3	0	-	-	0
2	0	-	-	0
1	1	-	-	1
Total	11	-	-	11

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
CentOS	10	-	-	10
Security Policy	1	-	-	1
Total	11	-	-	11

Vulnerabilities by Status



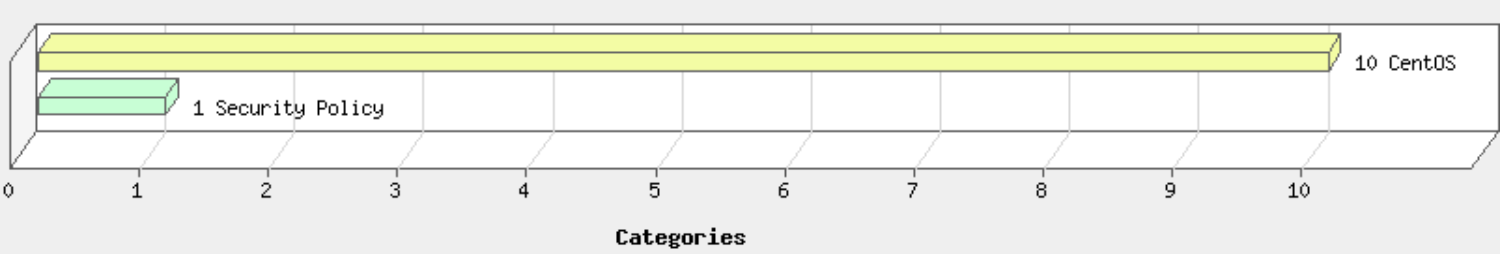
Vulnerabilities by Severity



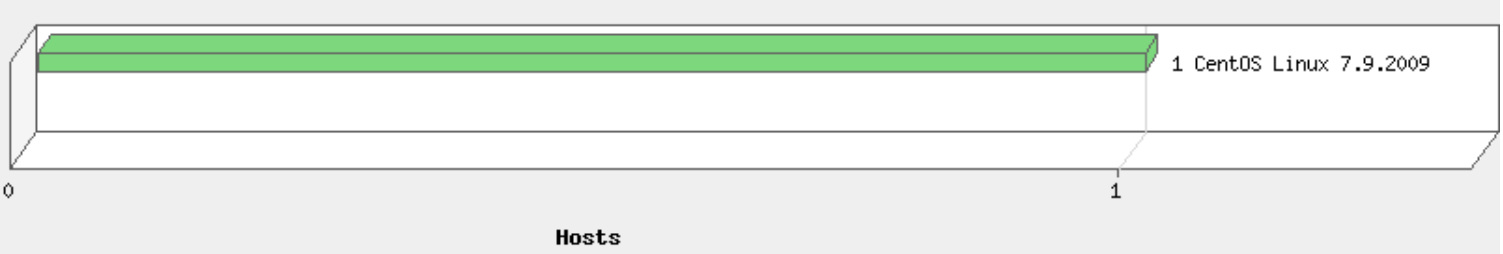
Information Gathered by Severity

There are no known vulnerabilities for this/these systems

Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.247.187.200 (de23p-wsopune-001.webcloud3.nic.in, -) CentOS Linux 7.9.2009

Host Identification Information	
IPs	
QG Host ID	bac37b54-0476-4b83-bf9e-5534a91227ac

Vulnerabilities Total	11	Security Risk	5.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	-	-	1
4	9	-	-	9
3	0	-	-	0
2	0	-	-	0
1	1	-	-	1
Total	11	-	-	11

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
CentOS	10	-	-	10
Security Policy	1	-	-	1
Total	11	-	-	11

Vulnerabilities (11)

5 CentOS Security Update for zlib (CESA-2023:1095) CVSS: 4 CVSS3.1: 8.5 Active

QID: 257227
Category: CentOS
Associated CVEs: CVE-2022-37434
Vendor Reference: CESA-2023:1095
Bugtraq ID: -
Service Modified: 09 Mar 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

CVSS Base: 5.4 [1]
CVSS Temporal: 4.0

CVSS3.1 Base: 9.8
CVSS3.1 Temporal: 8.5

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)
Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)
Times Detected: 264
Last Fixed: N/A

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

THREAT:
CentOS has released a security update for zlib security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:1095 (https://lists.centos.org/pipermail/centos-announce/2023-March/086387.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:1095: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-March/086387.html)

RESULTS:

Package	Installed Version	Required Version
zlib	1.2.7-20.el7_9.x86_64	1.2.7-21.el7_9
zlib-devel	1.2.7-20.el7_9.x86_64	1.2.7-21.el7_9
zlib	1.2.7-20.el7_9.x86_64	1.2.7-21.el7_9

4 CentOS Security Update for nss (CESA-2023:1332)

CVSS: 4 CVSS3.1: 7.5 Active

QID:	257230	CVSS Base:	5.4 [1]
Category:	CentOS	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-0767		
Vendor Reference:	CESA-2023:1332		
Bugtraq ID:	-		
Service Modified:	12 May 2023	CVSS3.1 Base:	8.6 [1]
User Modified:	-	CVSS3.1 Temporal:	7.5
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 31 Mar 2023 02:54:47 AM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 208

Last Fixed: N/A

CVSS Environment:

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

THREAT:

CentOS has released a security update for nss security update to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to CentOS security advisory CESA-2023:1332 (https://lists.centos.org/pipermail/centos-announce/2023-March/086393.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:1332: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-March/086393.html)

RESULTS:

Package	Installed Version	Required Version
nss-sysinit	3.79.0-4.el7_9.x86_64	3.79.0-5.el7_9
nss	3.79.0-4.el7_9.x86_64	3.79.0-5.el7_9
nss-tools	3.79.0-4.el7_9.x86_64	3.79.0-5.el7_9
nss	3.79.0-4.el7_9.x86_64	3.79.0-5.el7_9

4 CentOS Security Update for libXpm (CESA-2023:0377)

CVSS: 4 CVSS3.1: 7.7 Active

QID:	257211	CVSS Base:	5.4 [1]
Category:	CentOS	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-4883		
Vendor Reference:	CESA-2023:0377		
Bugtraq ID:	-		
Service Modified:	17 Feb 2023	CVSS3.1 Base:	8.8
User Modified:	-	CVSS3.1 Temporal:	7.7
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 264

Last Fixed: N/A

CVSS Environment:

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

THREAT:
CentOS has released a security update for libXpm security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:0377 (https://lists.centos.org/pipermail/centos-announce/2023-January/086364.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:0377: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-January/086364.html)

RESULTS:

Package	Installed Version	Required Version
libXpm	3.5.12-1.el7.x86_64	3.5.12-2.el7_9
libXpm	3.5.12-1.el7.x86_64	3.5.12-2.el7_9

4 CentOS Security Update for kernel (CESA-2023:1091) CVSS: 3.4 CVSS3.1: 6.8 Active

QID:	257226	CVSS Base:	4.6
Category:	CentOS	CVSS Temporal:	3.4
Associated CVEs:	CVE-2022-42703, CVE-2018-13405, CVE-2021-4037, CVE-2022-4378		
Vendor Reference:	CESA-2023:1091		
Bugtraq ID:	-		
Service Modified:	09 Mar 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 264

Last Fixed: N/A

CVSS Environment:

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

THREAT:
CentOS has released a security update for kernel security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:1091 (https://lists.centos.org/pipermail/centos-announce/2023-March/086390.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:1091: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-March/086390.html)

RESULTS:

Package	Installed Version	Required Version
kernel-headers	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7
python-perf	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.6.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.49.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.53.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.11.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel-tools	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel-tools-libs	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.6.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.49.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.53.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.11.1.el7.x86_64	3.10.0-1160.88.1.el7
kernel	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.88.1.el7

4 CentOS Security Update for bind (CESA-2023:0402)

CVSS: 3 CVSS3.1: 5.9 Active

QID:	257214	CVSS Base:	4.0
Category:	CentOS	CVSS Temporal:	3.0
Associated CVEs:	CVE-2022-2795, CVE-2021-25220		
Vendor Reference:	CESA-2023:0402		
Bugtraq ID:	-		
Service Modified:	17 May 2023	CVSS3.1 Base:	6.8
User Modified:	-	CVSS3.1 Temporal:	5.9
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)
Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)
Times Detected: 264
Last Fixed: N/A

CVSS Environment:

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

THREAT:
CentOS has released a security update for bind security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:0402 (https://lists.centos.org/pipermail/centos-announce/2023-January/086358.html) for updates and patch information.
Patch:

Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:0402: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-January/086358.html)

RESULTS:

Package	Installed Version	Required Version
bind-libs	9.11.4-26.P2.el7_9.10.x86_64	9.11.4-26.P2.el7_9.13
bind-libs-lite	9.11.4-26.P2.el7_9.10.x86_64	9.11.4-26.P2.el7_9.13
bind-export-libs	9.11.4-26.P2.el7_9.10.x86_64	9.11.4-26.P2.el7_9.13
bind-license	9.11.4-26.P2.el7_9.10.noarch	9.11.4-26.P2.el7_9.13
bind-utils	9.11.4-26.P2.el7_9.10.x86_64	9.11.4-26.P2.el7_9.13

4 CentOS Security Update for kernel (CESA-2023:0399)

CVSS: 1.6 CVSS3.1: 7.2 Active

QID:	257210	CVSS Base:	1.9
Category:	CentOS	CVSS Temporal:	1.6
Associated CVEs:	CVE-2017-5715, CVE-2021-26401, CVE-2022-2964		
Vendor Reference:	CESA-2023:0399		
Bugtraq ID:	-		
Service Modified:	12 May 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	7.2
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 264

Last Fixed: N/A

CVSS Environment:

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

THREAT:
CentOS has released a security update for kernel security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:0399 (https://lists.centos.org/pipermail/centos-announce/2023-January/086370.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:0399: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-January/086370.html)

RESULTS:

Package	Installed Version	Required Version
python-perf	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel-tools-libs	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.6.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.49.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.53.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.11.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel-headers	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel-tools	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7

kernel	3.10.0-1160.6.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.49.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.53.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.11.1.el7.x86_64	3.10.0-1160.83.1.el7
kernel	3.10.0-1160.76.1.el7.x86_64	3.10.0-1160.83.1.el7

4 CentOS Security Update for sudo (CESA-2023:0291)

CVSS: 4 CVSS3.1: 6.8 Active

QID:	257216	CVSS Base:	5.4 [1]
Category:	CentOS	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-22809		
Vendor Reference:	CESA-2023:0291		
Bugtraq ID:	-		
Service Modified:	31 Jan 2023	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 15 Mar 2023 07:26:45 PM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 264

Last Fixed: N/A

CVSS Environment:

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

THREAT:

CentOS has released a security update for sudo security update to fix the vulnerabilities.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Refer to CentOS security advisory CESA-2023:0291 (https://lists.centos.org/pipermail/centos-announce/2023-January/086363.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:0291: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-January/086363.html)

RESULTS:

Package	Installed Version	Required Version
sudo	1.8.23-10.el7_9.2.x86_64	1.8.23-10.el7_9.3
sudo	1.8.23-10.el7_9.2.x86_64	1.8.23-10.el7_9.3

4 CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2023:1335)

CVSS: 4 CVSS3.1: 6.4 Active

QID:	257231	CVSS Base:	5.4 [1]
Category:	CentOS	CVSS Temporal:	4.0
Associated CVEs:	CVE-2023-0286		
Vendor Reference:	CESA-2023:1335		
Bugtraq ID:	-		
Service Modified:	23 Mar 2023	CVSS3.1 Base:	7.4
User Modified:	-	CVSS3.1 Temporal:	6.4
Edited:	No		

PCI Vuln: Yes
Ticket State:

First Detected: 31 Mar 2023 02:54:47 AM (GMT+0530)
Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)
Times Detected: 208
Last Fixed: N/A

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

THREAT:
CentOS has released a security update for openssl security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2023:1335 (https://lists.centos.org/pipermail/centos-announce/2023-March/086392.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2023:1335: centos 7 (https://lists.centos.org/pipermail/centos-announce/2023-March/086392.html)

RESULTS:

Package	Installed Version	Required Version
openssl-libs	1.0.2k-25.el7_9.x86_64	1.0.2k-26.el7_9
openssl	1.0.2k-25.el7_9.x86_64	1.0.2k-26.el7_9
openssl-devel	1.0.2k-25.el7_9.x86_64	1.0.2k-26.el7_9
openssl	1.0.2k-25.el7_9.x86_64	1.0.2k-26.el7_9

4 CentOS Security Update for krb5 (CESA-2022:8640)

CVSS: 4 CVSS3.1: 7.7 Active

QID: 257203
Category: CentOS
Associated CVEs: CVE-2022-42898
Vendor Reference: CESA-2022:8640
Bugtraq ID: -
Service Modified: 06 Jan 2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State: Open

CVSS Base: 5.4 [1]
CVSS Temporal: 4.0

CVSS3.1 Base: 8.8
CVSS3.1 Temporal: 7.7

First Detected: 07 Dec 2022 10:22:08 PM (GMT+0530)
Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)
Times Detected: 666
Last Fixed: N/A

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

Availability Requirement: -

THREAT:
CentOS has released a security update for krb5 security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2022:8640 (https://lists.centos.org/pipermail/centos-announce/2022-November/073665.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2022:8640: centos 7 (https://lists.centos.org/pipermail/centos-announce/2022-November/073665.html)

RESULTS:

Package	Installed Version	Required Version
libkadm5	1.15.1-54.el7_9.x86_64	1.15.1-55.el7_9
krb5-devel	1.15.1-54.el7_9.x86_64	1.15.1-55.el7_9
krb5-libs	1.15.1-54.el7_9.x86_64	1.15.1-55.el7_9

4 CentOS Security Update for device-mapper-multipath Security Update (CESA-2022:7186) CVSS: 4 CVSS3.1: 6.8 Active

QID:	257206	CVSS Base:	5.4 [1]
Category:	CentOS	CVSS Temporal:	4.0
Associated CVEs:	CVE-2022-41974		
Vendor Reference:	CESA-2022:7186		
Bugtraq ID:	-		
Service Modified:	01 Dec 2022	CVSS3.1 Base:	7.8
User Modified:	-	CVSS3.1 Temporal:	6.8
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			

First Detected: 07 Dec 2022 10:22:08 PM (GMT+0530)
Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)
Times Detected: 666
Last Fixed: N/A

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

THREAT:
CentOS has released a security update for device-mapper-multipath Security Update security update to fix the vulnerabilities.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Refer to CentOS security advisory CESA-2022:7186 (https://lists.centos.org/pipermail/centos-announce/2022-November/073661.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2022:7186: centos 7 (https://lists.centos.org/pipermail/centos-announce/2022-November/073661.html)

RESULTS:

Package	Installed Version	Required Version

kpartx	0.4.9-135.el7_9.x86_64	0.4.9-136.el7_9

1 World-Writable Directories Should Have Their Sticky Bits Set — CVSS: 0 CVSS3.1: - Active

QID:	105146	CVSS Base:	0.0 [1]
Category:	Security Policy	CVSS Temporal:	0.0
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	12 May 2023	CVSS3.1 Base:	-
User Modified:	-	CVSS3.1 Temporal:	-
Edited:	No		
PCI Vuln:	No		
Ticket State:	Open		

First Detected: 17 Jan 2022 07:18:06 PM (GMT+0530)

Last Detected: 29 May 2023 04:09:04 AM (GMT+0530)

Times Detected: 2078

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:

/var/www/html/dhanush_dev/IRLA
/var/www/html/uploaded/json

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.