Qualys. Cloud Platform

National Informatics Centre

10.153.153.131

August 03, 2023

Report Summary	
User Name:	VA ADMIN NIC
Login Name:	nc_rt
Company:	NIC
User Role:	Manager
Address:	A-Block,Lodhi Rd,CGO Complex
City:	New Delhi
State:	Delhi
Zip:	110003
Country:	India
Created:	08/03/2023 at 11:07:50 AM (GMT+0530)
Template Title:	NIC
Asset Groups:	-
IPs:	10.153.153.131
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 08/03/2023
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	2	Security Risk (Avg)	4.0	Business Risk	36/100

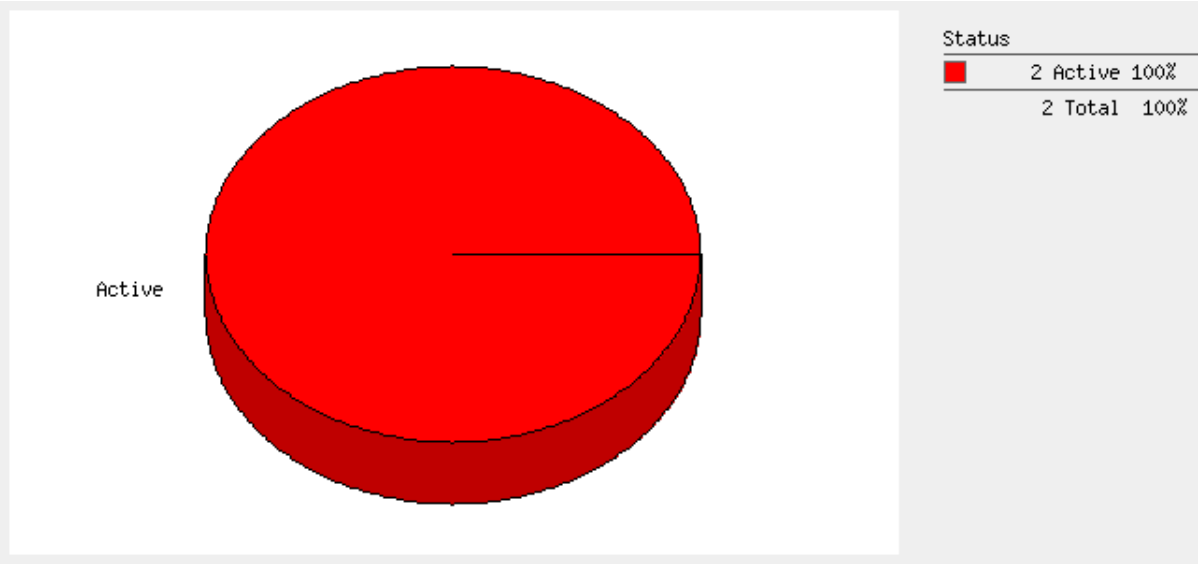
by Severity

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

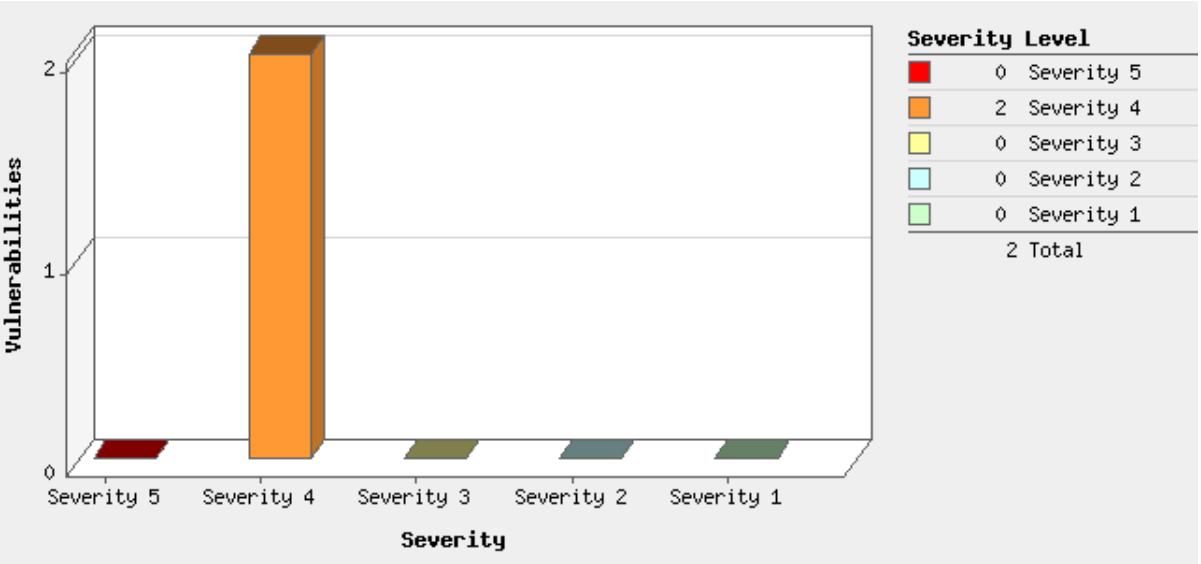
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
AlmaLinux	2	-	-	2
Total	2	-	-	2

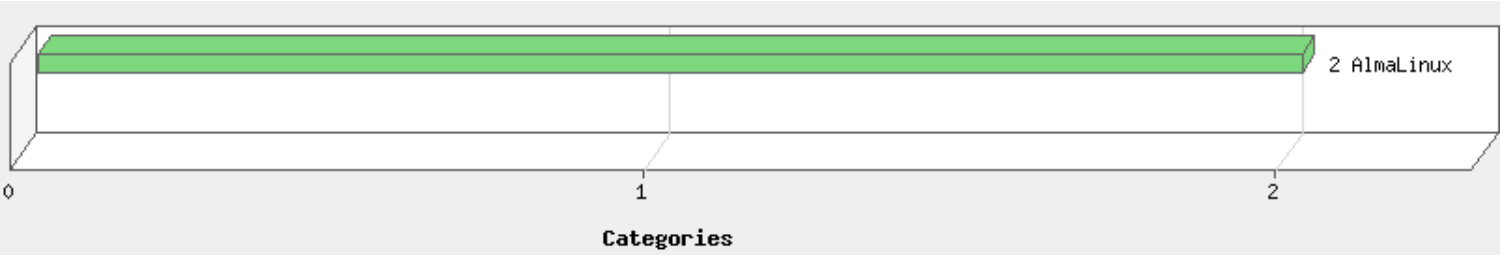
Vulnerabilities by Status



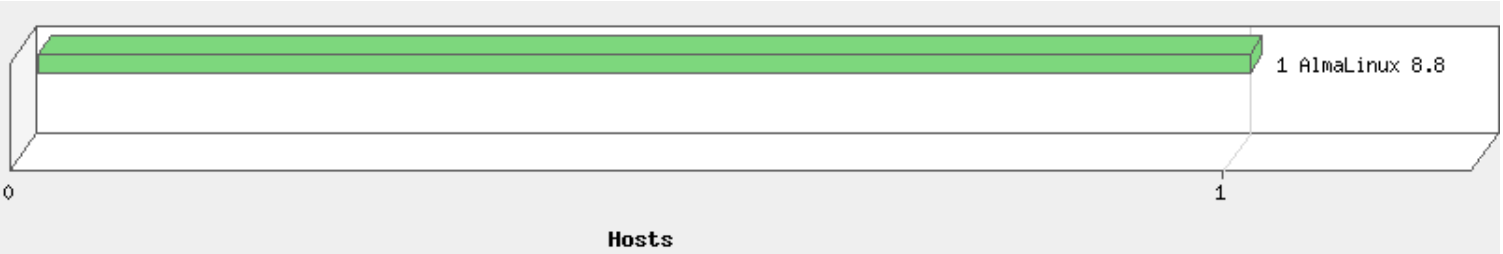
Vulnerabilities by Severity



Top 5 Vulnerable Categories



Operating Systems Detected



Detailed Results

10.153.153.131 (mtv9p-almarpo-001, -) AlmaLinux 8.8

Host Identification Information	
IPs	
QG Host ID	7b2c62a0-16a7-4ba1-b1f7-cc4e4ec742e9

Vulnerabilities Total	2	Security Risk	4.0

by Severity

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

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
AlmaLinux	2	-	-	2
Total	2	-	-	2

Vulnerabilities (2)

4 AlmaLinux Security Update for container-tools:4.0 (ALSA-2023:2802) Active

QID: 941090
Category: AlmaLinux
Associated CVEs: CVE-2022-30631, CVE-2022-30635, CVE-2022-32148, CVE-2022-41717, CVE-2022-30633, CVE-2022-1705, CVE-2022-32189, CVE-2023-0778, CVE-2022-1962, CVE-2022-30632, CVE-2022-28131, CVE-2022-27664, CVE-2022-30630, CVE-2022-2989
Vendor Reference: ALSA-2023:2802
Bugtraq ID: -
Service Modified: 06/02/2023
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 05/24/2023 at 01:25:56 AM (GMT+0530)
Last Detected: 08/03/2023 at 09:28:49 AM (GMT+0530)
Times Detected: 232

Last Fixed: N/A

THREAT:
AlmaLinux has released a security update for container-tools:4.0 to fix the vulnerabilities.

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

SOLUTION:
Refer to AlmaLinux security advisory ALSA-2023:2802 (https://errata.almalinux.org/8/ALSA-2023-2802.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ALSA-2023:2802: AlmaLinux (https://errata.almalinux.org/8/ALSA-2023-2802.html)

RESULTS:

Package	Installed Version	Required Version
crun	1.5-1.module_el8.7.0+3344+5bcd850f.x86_64	1.6-1.module_el8.8.0+3468+16b86c82
container-selinux	2.189.0-1.module_el8.7.0+3344+5bcd850f.noarch	2.199.0-1.module_el8.8.0+3468+16b86c82

4 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2023:2758) Active

QID:	941116
Category:	AlmaLinux
Associated CVEs:	CVE-2022-28131, CVE-2022-1705, CVE-2022-30632, CVE-2022-1962, CVE-2022-32148, CVE-2022-32189, CVE-2022-41717, CVE-2022-30631, CVE-2022-30635, CVE-2022-27664, CVE-2022-30630, CVE-2022-30633, CVE-2023-0778, CVE-2022-30629
Vendor Reference:	ALSA-2023:2758
Bugtraq ID:	-
Service Modified:	06/02/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 05/24/2023 at 07:02:56 AM (GMT+0530)
Last Detected: 08/03/2023 at 09:28:49 AM (GMT+0530)
Times Detected: 231
Last Fixed: N/A

THREAT:
AlmaLinux has released a security update for container-tools:rhel8 to fix the vulnerabilities.

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

SOLUTION:
Refer to AlmaLinux security advisory ALSA-2023:2758 (https://errata.almalinux.org/8/ALSA-2023-2758.html) for updates and patch information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
ALSA-2023:2758: AlmaLinux (https://errata.almalinux.org/8/ALSA-2023-2758.html)

RESULTS:

Package	Installed Version	Required Version
containernetworking-plugins	1.1.1-3.module_el8.6.0+3070+1510fbd1.x86_64	1.2.0-1.module_el8.8.0+3470+252b1910
udica	0.2.6-4.module_el8.6.0+3070+1510fbd1.noarch	0.2.6-20.module_el8.8.0+3470+252b1910
container-selinux	2.189.0-1.module_el8.7.0+3344+5bcd850f.noarch	2.205.0-2.module_el8.8.0+3557+7ba9cc13
criu	3.15-3.module_el8.6.0+2877+8e437bf5.x86_64	3.15-3.module_el8.7.0+3407+95aa0ca9
python3-podman	4.2.1-1.module_el8.7.0+3344+484dae7b.noarch	4.4.1-1.module_el8.8.0+3470+252b1910
crun	1.5-1.module_el8.7.0+3344+5bcd850f.x86_64	1.8.1-2.module_el8.8.0+3568+e8578284

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.