NeuVector

Full Lifecycle Container Security

Risk Report

In this Scan Summary Report

Summary 3

Severity Level Distribution 3

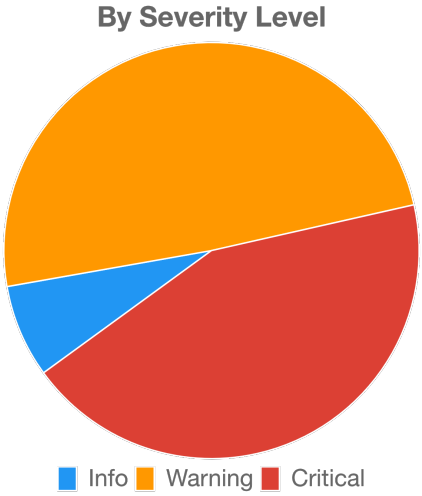
Scan Type Distribution 3

Details 4

Summary (Analyzed 4096 filtered records out of 4096 risk reports found from Feb 16, 2022 19:43:41 to Feb 17, 2022 15:41:18)

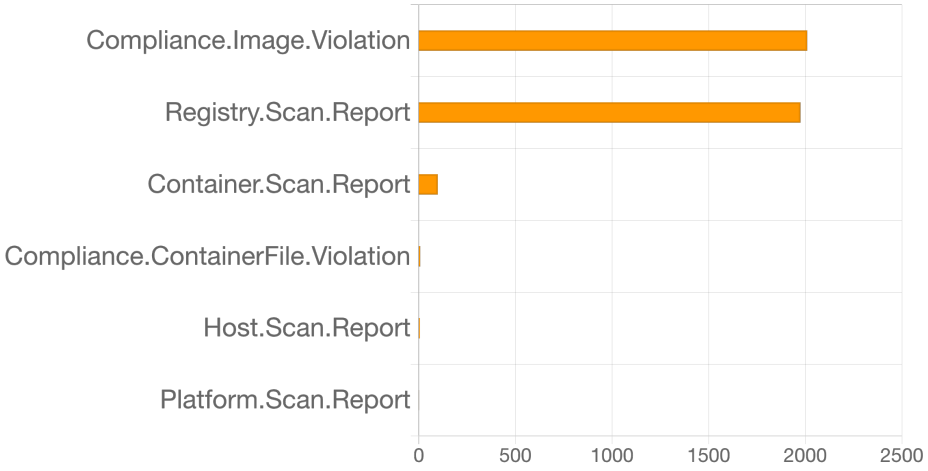
Severity Level Distribution

Info	296
Warning	2017
Critical	1783



Scan Type Distribution

Compliance.Image.Violation	2010
Registry.Scan.Report	1975
Container.Scan.Report	98
Compliance.ContainerFile.Violation	7
Host.Scan.Report	5
Platform.Scan.Report	1



Details

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1</td><td>Compliance.ContainerFile.Violation</td><td>Warning</td><td>Container : node-pod-65fd6ddcb6-wft6d
Node : gke-cluster-1-default-pool-d051acb1-5z3m</td><td>• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_dsa_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ecdsa_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ed25519_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_rsa_key contains Private.Key
• D.4.8 WARN - Total 19 files have setgid mode
• D.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 15:41:18</td></tr>
<tr><td>2</td><td>Container.Scan.Report</td><td>Critical</td><td>Container : node-pod-65fd6ddcb6-wft6d
Node : gke-cluster-1-default-pool-d051acb1-5z3m</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 405 Items)</td><td>• CVE-2016-1252
• CVE-2020-3810
• CVE-2020-27350
• .....
• (Total : 241 Items)</td></tr></table></td><td>Feb 17, 2022 15:41:01</td></tr>
<tr><td>3</td><td>Container.Scan.Report</td><td>Info</td><td>Container : node-pod-65fd6ddcb6-wft6d
Node : gke-cluster-1-default-pool-d051acb1-5z3m</td><td></td><td>Feb 17, 2022 15:40:53</td></tr>
<tr><td>4</td><td>Compliance.ContainerFile.Violation</td><td>Warning</td><td>Container : node-pod-65fd6ddcb6-cxmxm
Node : gke-cluster-1-default-pool-d051acb1-tztv</td><td>• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_dsa_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ecdsa_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ed25519_key contains Private.Key
• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_rsa_key contains Private.Key
• D.4.8 WARN - Total 19 files have setgid mode
• D.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 15:27:00</td></tr>
<tr><td>5</td><td>Container.Scan.Report</td><td>Critical</td><td>Container : node-pod-65fd6ddcb6-cxmxm
Node : gke-cluster-1-default-pool-d051acb1-tztv</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 405 Items)</td><td>• CVE-2016-1252
• CVE-2020-3810
• CVE-2020-27350
• .....
• (Total : 241 Items)</td></tr></table></td><td>Feb 17, 2022 15:26:46</td></tr>
<tr><td>6</td><td>Container.Scan.Report</td><td>Info</td><td>Container : node-pod-65fd6ddcb6-cxmxm
Node : gke-cluster-1-default-pool-d051acb1-tztv</td><td></td><td>Feb 17, 2022 15:26:22</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
7	Compliance.ContainerFile.Violation	Warning	**Container** : nginx-pod-b965fcc45-gdb4p **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	• nv.nginx-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssl/private/ssl-cert-snakeoil.key contains Private.Key • D.4.8 WARN - Total 18 files have setgid mode • D.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 15:09:47
8	Container.Scan.Report	Critical	**Container** : nginx-pod-b965fcc45-gdb4p **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845	Feb 17, 2022 15:09:34
9	Compliance.ContainerFile.Violation	Warning	**Container** : node-pod-65fd6ddcb6-qmszw **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_dsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ecdsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ed25519_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_rsa_key contains Private.Key • D.4.8 WARN - Total 19 files have setgid mode • D.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 15:07:40
10	Container.Scan.Report	Info	**Container** : node-pod-65fd6ddcb6-qmszw **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 15:07:13
11	Compliance.ContainerFile.Violation	Warning	**Container** : redis-pod-65c9cb584b-969tn **Node** : gke-cluster-1-default-pool-d051acb1-tztv	• D.4.8 WARN - Total 16 files have setgid mode • D.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 15:01:50
12	Container.Scan.Report	Critical	**Container** : redis-pod-65c9cb584b-969tn **Node** : gke-cluster-1-default-pool-d051acb1-tztv	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2018-12886 • CVE-2018-12886 • ..... • (Total : 48 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 27 Items)	Feb 17, 2022 15:01:37
13	Container.Scan.Report	Info	**Container** : redis-pod-65c9cb584b-969tn **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 15:01:31

ID	Name	Level	Location	Detail	Datetime
14	Compliance.ContainerFile.Violation	Warning	**Container** : c9158fde06ca1eb226353506898838910a8e994ff83f14d1e51bacec2ccc61f8 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_dsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ecdsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ed25519_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_rsa_key contains Private.Key • D.4.8 WARN - Total 10 files have setgid mode • D.4.8 WARN - Total 12 files have setuid mode	Feb 17, 2022 14:09:06
15	Container.Scan.Report	Critical	**Container** : node-pod-75c8bdfb87-2knhv **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 405 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 241 Items)	Feb 17, 2022 14:08:54
16	Container.Scan.Report	Info	**Container** : node-pod-75c8bdfb87-2knhv **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 14:08:30
17	Compliance.ContainerFile.Violation	Warning	**Container** : node-pod-75c8bdfb87-bl8f9 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	• nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_dsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ecdsa_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_ed25519_key contains Private.Key • nv.node-pod.demo/D.4.10 WARN - Ensure secrets are not stored in container images - File /etc/ssh/ssh_host_rsa_key contains Private.Key • D.4.8 WARN - Total 19 files have setgid mode • D.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 13:57:54
18	Container.Scan.Report	Critical	**Container** : node-pod-75c8bdfb87-bl8f9 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 405 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 241 Items)	Feb 17, 2022 13:57:31
19	Container.Scan.Report	Info	**Container** : node-pod-75c8bdfb87-bl8f9 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 13:57:21

ID	Name	Level	Location	Detail	Datetime
20	Container.Scan.Report	Info	**Container** : nginx-pod-b965fcc45-nptww **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 12:43:51
21	Container.Scan.Report	Info	**Container** : node-pod-75c8bdfb87-tlltg **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 12:16:02
22	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
23	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
24	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
25	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
26	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>27</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>28</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>29</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>30</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>31</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>32</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
33	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
34	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
35	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
36	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
37	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
38	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
39	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>40</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>41</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>42</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>43</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>44</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>45</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>46</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
47	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
48	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
49	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
50	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
51	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
52	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>53</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>54</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>55</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>56</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>57</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>58</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
59	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
60	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
61	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
62	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
63	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
64	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
65	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>66</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>67</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>68</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>69</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>70</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>71</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>72</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>73</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>74</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>75</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>76</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>77</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
78	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
79	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
80	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
81	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
82	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
83	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
84	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
85	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
86	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
87	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
88	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
89	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
90	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
91	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
92	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
93	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
94	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
95	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
96	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
97	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
98	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
99	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
100	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
101	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
102	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
103	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
104	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
105	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
106	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
107	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
108	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
109	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
110	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
111	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
112	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
113	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
114	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
115	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
116	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
117	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
118	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>119</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>120</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>121</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>122</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>123</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
124	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
125	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
126	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
127	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
128	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
129	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
130	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>131</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>132</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>133</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>134</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>135</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>136</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>137</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>138</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>139</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>140</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>141</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>142</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
143	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
144	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
145	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
146	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
147	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
148	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
149	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
150	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
151	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
152	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
153	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
154	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
155	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
156	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>157</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>158</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>159</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>160</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>161</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>162</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>163</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>164</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>165</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>166</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>167</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>168</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>169</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>170</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>171</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>172</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>173</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>174</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>175</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>176</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>177</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>178</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>179</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
180	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
181	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
182	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
183	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
184	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
185	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
186	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
187	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
188	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
189	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
190	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
191	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
192	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
193	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
194	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
195	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
196	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
197	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
198	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
199	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>200</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>201</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>202</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>203</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>204</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>205</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>206</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>207</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>208</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>209</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>210</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>211</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>212</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
213	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
214	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
215	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
216	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
217	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
218	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
219	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
220	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
221	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
222	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
223	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
224	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
225	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
226	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>227</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>228</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>229</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>230</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>231</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>232</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
233	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
234	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
235	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
236	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
237	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
238	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
239	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
240	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
241	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
242	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
243	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
244	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
245	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
246	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
247	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
248	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
249	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
250	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
251	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
252	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
253	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
254	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
255	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
256	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
257	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
258	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
259	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>260</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>261</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>262</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>263</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>264</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>265</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>266</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>267</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>268</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>269</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>270</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>271</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>272</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>273</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>274</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>275</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>276</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>277</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>278</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>279</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>280</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>281</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>282</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>283</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
284	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
285	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
286	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
287	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
288	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
289	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
290	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>291</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>292</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>293</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>294</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>295</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>296</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
297	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
298	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
299	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
300	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
301	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
302	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
303	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>304</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>305</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>306</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>307</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>308</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>309</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>310</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>311</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>312</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>313</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>314</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>315</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>316</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>317</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>318</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>319</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>320</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>321</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>322</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>323</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>324</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>325</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>326</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>327</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>328</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
329	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
330	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
331	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
332	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
333	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
334	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
335	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>336</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>337</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>338</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>339</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>340</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>341</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>342</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>343</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>344</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>345</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>346</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>347</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>348</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>349</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>350</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>351</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>352</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>353</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>354</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>355</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>356</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>357</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>358</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>359</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
360	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
361	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
362	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
363	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
364	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
365	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
366	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
367	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
368	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
369	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
370	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
371	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
372	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>373</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>374</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>375</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>376</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>377</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>378</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>379</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>380</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>381</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>382</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>383</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>384</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>385</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>386</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>387</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>388</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>389</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>390</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>391</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>392</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>393</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>394</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>395</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>396</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
397	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
398	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
399	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
400	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
401	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
402	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
403	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
404	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
405	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
406	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
407	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
408	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
409	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
410	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
411	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
412	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
413	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
414	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
415	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
416	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

ID	Name	Level	Location	Detail	Datetime
417	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
418	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
419	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
420	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
421	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
422	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
423	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>424</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>425</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>426</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>427</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>428</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>429</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>Base OS : debian:9
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2017-12613
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 1635 Items)</td><td>• CVE-2020-27350
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 1494 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:59</td></tr>
<tr><td>430</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/api_server:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 279 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:59</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
431	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
432	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:53:59
433	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:59
434	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
435	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
436	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
437	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
438	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
439	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
440	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
441	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
442	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
443	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
444	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
445	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
446	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
447	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
448	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
449	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>450</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>451</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>452</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>453</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>454</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>455</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>456</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>457</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>458</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>459</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>460</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>461</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>462</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>463</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>464</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>465</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>466</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>467</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>468</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>469</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>470</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>471</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>472</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>473</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
474	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
475	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
476	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
477	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
478	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
479	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>480</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>481</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>482</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>483</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>484</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>485</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>486</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>487</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>488</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>489</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>490</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>491</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>492</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>493</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>494</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>495</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>496</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>497</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
498	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
499	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
500	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
501	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
502	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
503	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>504</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>505</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>506</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>507</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>508</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>509</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>510</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>511</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>512</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>513</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>514</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>515</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>516</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>517</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>518</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>519</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>520</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>521</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
522	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
523	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
524	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
525	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
526	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
527	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>528</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>529</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>530</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>531</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>532</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>533</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>534</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>535</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>536</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>537</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>538</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>539</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>540</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>541</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>542</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>543</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>544</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>545</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
546	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
547	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
548	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
549	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
550	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
551	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>552</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>553</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>554</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>555</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>556</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>557</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>558</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>559</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>560</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>561</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>562</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>563</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>564</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>565</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>566</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>567</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>568</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>569</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>570</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>571</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>572</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>573</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>574</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>575</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>576</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>577</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>578</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>579</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>580</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>581</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>582</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>583</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>584</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>585</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>586</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>587</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>588</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>589</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>590</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>591</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>592</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>593</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>594</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>595</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>596</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>597</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>598</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>599</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>600</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>601</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>602</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>603</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>604</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>605</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>606</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>607</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>608</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>609</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>610</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>611</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>612</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>613</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>614</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>615</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>616</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>617</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
618	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
619	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
620	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
621	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
622	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
623	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>624</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>625</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>626</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>627</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>628</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>629</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>630</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>631</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>632</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>633</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>634</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>635</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
636	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
637	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
638	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
639	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
640	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
641	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>642</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>643</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>644</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>645</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>646</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>647</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>648</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>649</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>650</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>651</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>652</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>653</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
654	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
655	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
656	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
657	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
658	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
659	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
660	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
661	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
662	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
663	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
664	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
665	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>666</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>667</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>668</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>669</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>670</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>671</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
672	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
673	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
674	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
675	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
676	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
677	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>678</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>679</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>680</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>681</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>682</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>683</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>684</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>685</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>686</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>687</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>688</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>689</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
690	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
691	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
692	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
693	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
694	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
695	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
696	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
697	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
698	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
699	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
700	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
701	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>702</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>703</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>704</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>705</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>706</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>707</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
708	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
709	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
710	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
711	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
712	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
713	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
714	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
715	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
716	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
717	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
718	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
719	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>720</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>721</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>722</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>723</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>724</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>725</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
726	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
727	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
728	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
729	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
730	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
731	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
732	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
733	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
734	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
735	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
736	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
737	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>738</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>739</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>740</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>741</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>742</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>743</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>744</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>745</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>746</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>747</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>748</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>749</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
750	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
751	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
752	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
753	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
754	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
755	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>756</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>757</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>758</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>759</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>760</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>761</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
762	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
763	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
764	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
765	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
766	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
767	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>768</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>769</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>770</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>771</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>772</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>773</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>774</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>775</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>776</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>777</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>778</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>779</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>780</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>781</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>782</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>783</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>784</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>785</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>786</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>787</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>788</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>789</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>790</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>791</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
792	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
793	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
794	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
795	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
796	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
797	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
798	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
799	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
800	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
801	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
802	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
803	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
804	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
805	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
806	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
807	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
808	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
809	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
810	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
811	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
812	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
813	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
814	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
815	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>816</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>817</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>818</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>819</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>820</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>821</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>822</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>823</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>824</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>825</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>826</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>827</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>828</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>829</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>830</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>831</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>832</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey</li><li>I.4.8 WARN - Total 18 files have setgid mode</li><li>I.4.8 WARN - Total 10 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:53:24</td></tr>
<tr><td>833</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/swarm_nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2021-23017</li><li>CVE-2019-9511</li><li>CVE-2017-7529</li></ul></td><td><ul><li>CVE-2018-16845</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:53:24</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
834	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
835	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
836	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
837	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
838	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
839	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
840	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
841	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
842	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
843	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:53:24
844	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24
845	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:53:24

ID	Name	Level	Location	Detail	Datetime
846	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:49:23
847	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:49:23
848	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:49:23
849	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:49:23
850	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
851	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
852	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
853	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
854	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
855	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
856	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
857	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
858	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
859	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
860	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
861	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
862	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
863	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
864	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
865	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
866	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
867	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
868	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
869	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
870	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
871	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
872	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
873	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
874	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
875	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
876	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
877	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
878	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
879	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
880	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
881	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
882	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
883	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
884	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
885	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
886	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
887	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
888	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
889	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
890	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
891	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
892	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
893	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
894	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
895	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
896	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
897	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
898	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
899	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
900	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
901	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
902	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
903	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
904	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
905	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
906	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
907	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
908	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
909	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
910	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
911	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
912	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
913	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
914	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
915	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
916	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
917	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
918	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
919	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
920	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
921	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
922	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
923	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
924	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
925	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
926	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
927	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
928	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
929	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
930	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
931	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
932	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
933	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
934	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
935	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
936	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
937	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
938	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
939	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
940	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
941	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
942	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
943	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
944	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
945	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
946	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
947	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
948	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
949	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
950	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
951	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
952	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
953	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
954	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
955	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
956	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
957	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
958	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
959	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
960	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
961	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
962	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
963	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
964	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
965	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
966	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
967	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
968	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
969	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
970	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
971	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
972	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
973	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
974	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
975	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
976	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
977	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
978	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
979	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
980	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
981	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
982	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
983	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
984	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
985	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
986	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
987	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
988	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
989	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
990	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
991	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
992	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
993	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
994	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
995	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
996	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
997	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
998	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
999	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1000	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1001	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1002	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1003	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1004	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1005	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1006	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1007	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1008	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1009	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1010	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1011	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1012	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1013	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1014	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1015	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1016	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1017	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1018	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1019	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1020	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1021	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1022	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1023	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1024	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1025	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1026	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1027	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1028	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1029	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1030	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1031	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1032	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1033	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1034	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1035	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1036	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1037	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1038	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1039	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1040	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1041	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1042	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1043	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1044	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1045	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1046	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1047	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1048	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1049	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1050	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1051	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1052	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1053	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1054	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1055	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1056	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1057	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1058	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1059	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1060	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1061	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1062	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1063	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1064	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1065	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1066	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1067	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1068	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1069	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1070	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1071	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1072	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1073	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1074	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1075	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1076	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1077	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1078	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1079	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1080	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1081	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1082	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1083	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1084	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1085	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1086	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1087	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1088	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1089	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1090	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1091	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1092	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1093	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1094	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1095	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1096	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1097	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1098	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1099	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1100	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1101	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1102	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1103	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1104	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1105	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1106	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1107	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1108	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1109	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1110	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1111	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1112	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1113	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1114	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1115	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1116	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1117	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1118	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1119	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1120	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1121	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1122	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1123	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1124	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1125	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1126	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1127	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1128	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1129	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1130	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1131	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1132	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1133	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1134	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1135	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1136	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1137	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1138	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1139	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1140	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1141	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1142	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1143	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1144	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1145	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1146	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1147	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1148	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1149	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1150	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1151	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1152	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1153	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1154	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1155	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1156	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1157	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1158	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1159	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1160	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1161	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1162	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1163	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1164	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1165	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1166	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1167	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1168	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1169	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1170	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1171	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1172	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1173	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1174	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1175	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1176	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1177	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1178	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1179	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1180	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1181	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1182	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1183	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1184	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1185	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1186	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1187	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1188	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1189	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1190	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1191	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1192	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1193	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1194	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1195	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1196	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1197	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1198	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1199	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1200	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1201	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1202	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1203	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1204	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1205	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1206	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1207	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1208	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1209	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1210	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1211	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1212	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1213	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1214	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1215	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1216	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1217	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1218	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1219	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1220	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1221	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1222	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1223	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1224	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1225	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1226	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1227	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1228	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1229	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1230	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1231	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1232	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1233	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1234	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1235	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1236	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1237	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1238	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1239	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1240	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1241	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1242	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1243	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1244	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1245	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1246	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1247	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1248	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1249	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1250	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1251	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1252	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1253	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1254	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1255	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1256	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1257	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1258	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1259	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1260	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1261	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:48:53
1262	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53
1263	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:48:53

ID	Name	Level	Location	Detail	Datetime
1264	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1265	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1266	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1267	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1268	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1269	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1270	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1271	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1272	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1273	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1274	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1275	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1276	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1277	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1278	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1279	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1280	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1281	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1282	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1283	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1284	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1285	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1286	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1287	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1288	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1289</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1290</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1291</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1292</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1293</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1294</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1295</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1296</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1297</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1298</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1299</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1300</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1301</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1302</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1303</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1304</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1305</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1306</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1307</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1308</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1309	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1310	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1311	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1312	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1313	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1314	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1315	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1316	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1317	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1318	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1319</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1320</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1321</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1322</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1323</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1324	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1325	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1326	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1327	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1328	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1329	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1330	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1331	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1332	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1333	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1334</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1335</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1336</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1337</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1338</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1339</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1340</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1341</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1342</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1343</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1344</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1345</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1346</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1347</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1348</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1349</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1350</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1351</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1352</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1353</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1354</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1355</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1356</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1357</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1358</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1359</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1360</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1361</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1362</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1363</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1364</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1365</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1366</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1367</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1368</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1369	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1370	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1371	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1372	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1373	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1374	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1375	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1376	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1377	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1378	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1379	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1380	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1381	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1382	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1383	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1384	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1385	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1386	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1387	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1388	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1389	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1390	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1391	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1392	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1393	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1394</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1395</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1396</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1397</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1398</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1399</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1400</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1401</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1402</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1403</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1404	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1405	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1406	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1407	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1408	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1409	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1410	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1411	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1412	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1413	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1414</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1415</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1416</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1417</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1418</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1419</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1420</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1421</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1422</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1423</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1424	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1425	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1426	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1427	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1428	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1429	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1430	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1431	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1432	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1433	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1434	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1435	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1436	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1437	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1438	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1439</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1440</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1441</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1442</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1443</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1444	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1445	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1446	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1447	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1448	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1449	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1450	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1451	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1452	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1453	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1454	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1455	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1456	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1457	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1458	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1459	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1460	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1461	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1462	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1463	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1464</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1465</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1466</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1467</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1468</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1469	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1470	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1471	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1472	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1473	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1474</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1475</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1476</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1477</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1478</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1479	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1480	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1481	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1482	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1483	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1484	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1485	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1486	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1487	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1488	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1489	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1490	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1491	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1492	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1493	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1494	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1495	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1496	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1497	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1498	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1499	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1500	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1501	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1502	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1503	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1504</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1505</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1506</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1507</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1508</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1509	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1510	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1511	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1512	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1513</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1514</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1515</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1516</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1517</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1518</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1519</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1520</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1521</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1522</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1523	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1524	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1525	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1526	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1527	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1528</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1529</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1530</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1531</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1532</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1533</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1534</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1535</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1536</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1537</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1538	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1539	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1540	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1541	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1542	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1543	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1544	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1545	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1546	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1547	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1548</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1549</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1550</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1551</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1552</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1553	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1554	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1555	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1556	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1557	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1558	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1559	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1560	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1561	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1562	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1563	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1564	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1565	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1566	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1567	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1568	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1569	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1570	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1571	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1572</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1573</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1574</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1575</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1576</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1577</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1578</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1579</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1580</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1581</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1582</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1583</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1584</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1585</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1586</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1587	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1588	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1589	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1590	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1591	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1592</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1593</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1594</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1595</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1596</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1597</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1598</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1599</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1600</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1601</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1602</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1603</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1604</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1605</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1606</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1607	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1608	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1609	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1610	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1611	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1612	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1613	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1614	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1615	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1616	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1617</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1618</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1619</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1620</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1621</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1622</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1623</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1624</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1625</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1626</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1627	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1628	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1629	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1630	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1631	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1632	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1633	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1634	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1635	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1636	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1637	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1638	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1639	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1640	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1641	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1642</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1643</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1644</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1645</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1646</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1647	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1648	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1649	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1650	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1651	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1652</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1653</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1654</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1655</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1656</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1657	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1658	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1659	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1660	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1661	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1662	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1663	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1664	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1665	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1666	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1667</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1668</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1669</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1670</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1671</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1672</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1673</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1674</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1675</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1676</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1677	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1678	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1679	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1680	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1681	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1682</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1683</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1684</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1685</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1686</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1687	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1688	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1689	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1690	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1691	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1692</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1693</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1694</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1695</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1696</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1697</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1698</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1699</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1700</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1701</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1702</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1703</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1704</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1705</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1706</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1707</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1708</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1709</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1710</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1711</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1712</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1713</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1714</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1715</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1716</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1717</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1718</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1719</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1720</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1721</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1722	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1723	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1724	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1725	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1726	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1727	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1728	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1729	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1730	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1731	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1732</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1733</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1734</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1735</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1736</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1737</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1738</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1739</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1740</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1741</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1742	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1743	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1744	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1745	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1746	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1747	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1748	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1749	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1750	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1751	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1752</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1753</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1754</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1755</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1756</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1757</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1758</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1759</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1760</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1761</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1762	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1763	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1764	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1765	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1766	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1767	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1768	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1769	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1770	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1771	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1772	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1773	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1774	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1775	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1776	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1777	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1778	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1779	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1780	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1781	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1782</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1783</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1784</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1785</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1786</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1787	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1788	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1789	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1790	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1791	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1792	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1793	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1794	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1795	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1796	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1797</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1798</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1799</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1800</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1801</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1802</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1803</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1804</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1805</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1806</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1807</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1808</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1809</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1810</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1811</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1812	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1813	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1814	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1815	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1816	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1817</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1818</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1819</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1820</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1821</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1822</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1823</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1824</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1825</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1826</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1827	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1828	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1829	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1830	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1831	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1832	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1833	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1834	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1835	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1836	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1837	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1838	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1839	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1840	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1841	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1842</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1843</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1844</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1845</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1846</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1847	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1848	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1849	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1850	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1851	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1852</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1853</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1854</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1855</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1856</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1857	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1858	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1859	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1860	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1861	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1862</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1863</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1864</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1865</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1866</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1867	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1868	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1869	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1870	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1871	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1872	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1873	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1874	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1875	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1876	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1877	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1878	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1879	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1880	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1881	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1882</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1883</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1884</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1885</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1886</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1887	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1888	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1889	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1890	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1891	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1892	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1893	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1894	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1895	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1896	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1897	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1898	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1899	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1900	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1901	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1902	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1903	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1904	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1905	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1906	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1907	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1908	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1909	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1910	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1911	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1912	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1913	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1914	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1915	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1916	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1917	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1918	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1919	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1920	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1921	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1922	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1923	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1924	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1925	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1926	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1927	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1928	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1929	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1930	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1931	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1932</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1933</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1934</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1935</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1936</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1937	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1938	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1939	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1940	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1941	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1942</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1943</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1944</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1945</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1946</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1947	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1948	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1949	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1950	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1951	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1952</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1953</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1954</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1955</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1956</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1957	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1958	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1959	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1960	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1961	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1962	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1963	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1964	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1965	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1966	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1967	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1968	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1969	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1970	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1971	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1972	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1973	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1974	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1975	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1976	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1977</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1978</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1979</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1980</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1981</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
1982	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1983	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1984	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1985	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1986	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1987	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1988	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1989	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1990	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1991	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
1992	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1993	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1994	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
1995	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
1996	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>1997</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1998</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>1999</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2000</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2001</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2002	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2003	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2004	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2005	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2006	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2007	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2008	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2009	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2010	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2011	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2012	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2013	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2014	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2015	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2016	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2017	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2018	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2019	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2020	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2021	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2022</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2023</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2024</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2025</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2026</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2027</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2028</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2029</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2030</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2031</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2032	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2033	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2034	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2035	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2036	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2037	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2038	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2039	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2040	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2041	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2042</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2043</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2044</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2045</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2046</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2047	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2048	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2049	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2050	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2051	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2052	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2053	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2054	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2055	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2056	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2057	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2058	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2059	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2060	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2061	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2062</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2063</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2064</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2065</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2066</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2067	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2068	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2069	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2070	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2071	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2072	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2073	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2074	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2075	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2076	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51

ID	Name	Level	Location	Detail	Datetime
2077	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2078	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51
2079	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2016-1252 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:48:51
2080	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:48:51

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2081</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2082</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2083</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2084</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td><ul><li>I.4.1 WARN - Ensure a user for the container has been created</li><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /build/insecure_key.ppk contains privatekey</li><li>I.4.10 WARN - File /etc/insecure_key contains privatekey</li><li>I.4.10 WARN - File /build/insecure_key contains privatekey</li><li>I.4.8 WARN - Total 14 files have setgid mode</li><li>I.4.8 WARN - Total 14 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2085</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 394 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 236 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2086</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2087</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2088</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 394 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 236 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2089</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/dns_client2:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /build/insecure_key.ppk contains privatekey
• I.4.10 WARN - File /etc/insecure_key contains privatekey
• I.4.10 WARN - File /build/insecure_key contains privatekey
• I.4.8 WARN - Total 14 files have setgid mode
• I.4.8 WARN - Total 14 files have setuid mode</td><td>Feb 17, 2022 06:48:51</td></tr>
<tr><td>2090</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2091	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2092	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2093	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2094	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2095	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2096	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2097	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2098	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2099	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2100	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2101	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2102	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2103	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2104	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2105	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2106	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2107	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2108	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2109	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2110	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2111	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2112	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2113	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2114	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2115	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2116	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2117	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2118	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2119	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2120	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2121</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2122</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2123</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2124</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2125</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2126</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2127	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2128	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2129	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2130	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2131	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2132	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2133</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2134</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2135</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2136</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2137</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2138</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2139</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2140</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2141</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2142</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2143</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2144</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2145	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2146	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2147	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2148	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2149	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2150	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2151	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2152	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2153	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2154	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2155	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2156	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2157</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2158</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2159</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2160</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2161</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2162</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2163	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2164	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2165	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2166	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2167	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2168	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2169	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2170	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2171	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2172	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2173	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2174	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2175	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2176	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2177	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2178	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2179	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2180	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2181	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2182	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2183	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2184	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2185	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2186	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2187	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2188	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2189	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2190	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2191	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2192	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2193</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2194</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2195</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2196</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2197</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2198</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2199	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2200	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2201	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2202	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2203	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2204	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2205</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2206</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2207</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2208</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2209</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2210</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2211</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2212</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2213</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2214</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2215</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2216</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2217	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2218	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2219	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2220	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2221	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2222	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2223	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2224	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2225	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2226	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2227	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2228	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2229	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2230	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2231	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2232	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2233	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2234	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2235	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2236	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2237	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2238	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2239	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2240	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2241	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2242	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2243	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2244	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2245	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2246	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2247	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2248	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2249	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2250	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2251	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2252	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2253</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2254</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2255</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2256</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2257</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2258</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2259	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2260	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2261	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2262	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2263	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2264	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2265</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2266</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2267</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2268</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2269</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2270</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2271	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2272	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2273	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2274	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2275	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2276	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2277	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2278	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2279	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2280	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2281	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2282	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2283	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2284	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2285	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2286	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2287	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2288	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2289</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2290</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2291</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2292</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2293</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2294</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2295	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2296	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2297	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2298	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2299	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2300	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2301	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2302	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2303	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2304	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2305	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2306	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2307</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2308</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2309</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2310</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2311</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2312</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2313	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2314	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2315	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2316	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2317	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2318	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2319</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2320</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2321</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2322</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2323</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2324</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2325</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2326</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2327</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2328</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2329</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2330</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2331</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2332</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2333</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2334</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2335</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2336</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2337	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2338	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2339	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2340	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2341	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2342	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2343</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2344</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2345</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2346</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2347</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2348</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2349</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2350</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2351</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2352</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2353</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2354</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2355</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2356</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2357</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2358</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2359</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2360</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2361</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2362</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2363</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2364</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2365</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2366</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2367</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2368</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2369</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2370</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2371</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2372</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2373</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2374</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2375</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2376</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2377</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2378</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2379</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2380</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2381</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2382</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2383</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2384</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2385	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2386	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2387	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2388	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2389	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2390	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2391</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2392</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2393</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2394</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2395</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2396</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2397</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2398</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2399</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2400</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2401</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2402</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2403</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2404</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2405</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2406</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2407</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2408</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2409	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2410	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2411	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2412	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2413	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2414	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2415</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2416</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2417</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2418</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2419</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2420</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2421</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2422</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2423</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2424</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2425</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2426</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2427	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2428	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2429	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2430	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2431	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2432	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2433</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2434</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2435</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2436</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2437</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2438</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2439</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2440</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2441</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2442</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2443</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2444</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2445	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2446	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2447	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2448	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2449	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2450	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2451</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2452</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2453</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2454</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2455</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2456</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2457</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2458</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2459</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2460</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2461</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2462</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2463	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2464	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2465	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2466	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2467	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2468	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2469	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2470	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2471	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2472	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2473	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2474	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2475	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2476	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2477	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2478	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2479	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2480	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2481</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2482</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2483</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2484</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2485</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 17, 2022 06:48:33</td></tr>
<tr><td>2486</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2021-23017
• CVE-2019-9511
• CVE-2017-7529</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:33</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2487	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2488	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2489	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2490	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2491	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2492	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2493	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2494	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2495	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2496	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2497	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2498	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33

ID	Name	Level	Location	Detail	Datetime
2499	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2500	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2501	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2502	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2021-23017 • CVE-2019-9511 • CVE-2017-7529 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:33
2503	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:33
2504	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:25

ID	Name	Level	Location	Detail	Datetime
2505	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:25
2506	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:48:25
2507	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:48:25
2508	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2509	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2510	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2511	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2512	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2513	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2514	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2515	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2516	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2517	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2518	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2519	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2520	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2521	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2522	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2523	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2524	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2525	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2526	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2527	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2528	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2529	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2530	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2531	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2532	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2533	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2534	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2535	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2536	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2537	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2538	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2539	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2540	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2541	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2542	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2543	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2544	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2545	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2546	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2547	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2548	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2549	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2550	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2551	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2552	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2553	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2554</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2555</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2556</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2557</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2558</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2559</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2560	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2561	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2562	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2563	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2564	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2565	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2566	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2567	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2568	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2569	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2570	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2571	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2572	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2573</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2574</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2575</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2576</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2577</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2578</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2579</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2580	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2581	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2582	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2583	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2584	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2585	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2586	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2587	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2588	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2589	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2590	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2591	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2592	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2593	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2594	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2595	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2596	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2597	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2598	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2599	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2600	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2601	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2602	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2603	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2604	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2605	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2606	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2607	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2608	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2609	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2610	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2611</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2612</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2613</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2614</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2615</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2616</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2617	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2618	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2619	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2620	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2621	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2622	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2623	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2624	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2625	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2626	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2627	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2628	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2629	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2630	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2631	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2632	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2633	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2634	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2635	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2636	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2637	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2638	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2639	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2640	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2641	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2642	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2643	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2644	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2645	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2646	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2647	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2648	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2649	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2650	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2651	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2652	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2653	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2654	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2655	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2656	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2657	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2658	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2659	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2660	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2661	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2662	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2663	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2664	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2665	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2666	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2667</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2668</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2669</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2670</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>Base OS : ubuntu:18.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2018-19591
• CVE-2020-1751
• CVE-2018-11237
• .....
• (Total : 15 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2020-27350
• .....
• (Total : 18 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2671</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
<tr><td>2672</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/iodine:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.8 WARN - Total 7 files have setgid mode
• I.4.8 WARN - Total 8 files have setuid mode</td><td>Feb 17, 2022 06:48:23</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2673	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2674	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2675	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2676	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2677	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2678	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2679	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2680	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2681	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2682	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2683	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2684	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2685	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2686	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2687	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2688	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2689	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2690	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2691	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2692	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2693	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2694	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2695	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2696	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2697	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2698	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2699	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2700	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2701	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2702	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2703	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2704	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2705	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2706	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2707	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2708	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2709	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2710	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2711	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2712	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2713	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2714	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2715	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2716	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2717	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2718	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2719	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2720	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2721	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2722	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2723	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2724	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2725	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2726	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2727	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2728	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2729	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2730	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2731	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2732	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2733	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2734	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2735	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2736	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2737	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2738	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2739	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2740	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2741	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2742	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2743	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2744	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2745	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2746	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2747	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2748	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2749	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2750	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2751	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2752	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2753	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2754	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2755	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2756	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2757	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2758	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2759	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2760	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2761	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2762	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2763	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2764	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2765	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2766	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2767	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2768	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2769	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2770	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2771	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2772	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2773	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2774	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2775	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2776	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2777	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2778	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2779	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2780	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2781	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2782	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2783	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2784	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2785	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2786	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2787	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2788	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2789	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2790	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2791	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2792	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2793	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2794	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2795	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2796	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2797	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2798	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2799	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2800	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2801	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2802	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2803	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2804	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2805	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2806	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2807	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2808	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2809	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2810	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2811	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2812	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2813	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2814	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2815	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2816	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2817	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2818	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2819	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2820	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2821	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2822	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2823	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2824	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2825	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2826	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2827	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2828	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2829	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2830	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2831	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2832	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2833	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2834	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2835	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2836	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2837	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2838	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2839	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2840	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2841	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2842	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2843	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2844	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2845	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2846	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2847	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2848	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2849	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2850	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2851	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2852	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2853	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2854	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2855	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2856	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2857	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2858	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2859	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2860	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2861	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2862	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2863	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2864	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2865	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2866	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2867	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2868	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2869	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2870	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2871	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2872	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2873	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2874	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2875	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2876	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2877	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2878	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2879	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2880	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2881	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2882	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2883	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2884	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2885	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2886	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2887	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2888	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2889	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2890	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2891	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2892	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2893	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2894	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2895	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2896	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2897	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2898	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2899	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2900	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2901	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2902	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2903	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2904	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2905	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2906	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2907	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2908	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2909	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2910	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2911	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2912	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2913	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2914	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2915	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23

ID	Name	Level	Location	Detail	Datetime
2916	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2917	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2918	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23
2919	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2920	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-19591 • CVE-2020-1751 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:48:23
2921	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:48:23

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>2922</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>2923</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>2924</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>2925</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>2926</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
2927	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2928	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2929	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2930	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2931	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2932	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2933	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2934	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2935	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2936	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2937	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2938	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2939	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2940	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2941	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2942	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2943	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2944	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2945	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2946	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2947	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2948	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2949	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2950	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2951	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2952	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2953	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2954	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2955	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2956	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2957	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2958	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2959	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2960	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2961	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2962	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2963	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2964	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2965	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2966	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2967	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2968	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2969	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2970	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2971	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2972	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2973	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2974	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2975	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2976	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2977	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2978	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2979	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2980	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2981	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2982	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2983	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2984	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2985	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2986	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2987	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2988	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2989	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2990	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2991	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2992	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2993	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2994	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2995	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
2996	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2997	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
2998	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
2999	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3000	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3001	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3002</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3003</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3004</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3005</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3006</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3007</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3008</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3009</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3010</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3011</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3012	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3013	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3014	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3015	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3016	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3017	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3018	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3019	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3020	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3021	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3022	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3023	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3024	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3025	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3026	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3027	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3028	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3029	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3030	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3031	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3032	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3033	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3034	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3035	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3036	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3037	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3038	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3039	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3040	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3041	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3042	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3043	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3044	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3045	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3046	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3047	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3048	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3049	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3050	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3051	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3052	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3053	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3054	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3055	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3056	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3057	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3058	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3059	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3060	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3061	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3062	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3063	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3064	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3065</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3066</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3067</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3068</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3069</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3070</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3071	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3072	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3073	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3074	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3075	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3076	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3077	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3078	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3079	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3080	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3081	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3082	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3083	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3084	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3085	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3086	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3087	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3088	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3089	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3090	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3091	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3092	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3093	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3094	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3095	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3096	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3097	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3098	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3099	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3100</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3101</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3102</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3103</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3104</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3105	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3106	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3107	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3108	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3109	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3110	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3111	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3112	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3113	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3114	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3115	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3116	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3117	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3118	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3119	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3120	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3121	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3122	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3123	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3124	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3125	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3126	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3127	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3128	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3129	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3130	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3131	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3132	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3133	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3134	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3135	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3136	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3137	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3138	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3139	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3140	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3141	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3142	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3143	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3144	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3145</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3146</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3147</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3148</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3149</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3150</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3151</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3152</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3153</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3154</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3155</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3156	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3157	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3158	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3159	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3160	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3161	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3162	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3163	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3164	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3165	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3166	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3167	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3168	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3169	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3170	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3171	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3172	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3173	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3174	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3175	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3176	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3177	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3178	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3179	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3180	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3181	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3182	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3183	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3184	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3185	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3186	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3187	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3188	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3189	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3190	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3191	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3192	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3193	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3194	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3195	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3196	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3197	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3198	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3199	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3200	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3201	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3202	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3203	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3204	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3205	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3206	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3207	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3208	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3209	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3210	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3211	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3212	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3213	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3214	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3215	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3216	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3217	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3218	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3219	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3220	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3221	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3222</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3223</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3224</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3225</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3226</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3227</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3228	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3229	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3230	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3231	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3232	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3233</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3234</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3235</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3236</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3237</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3238	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3239	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3240	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3241	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3242	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3243	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3244	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3245	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3246	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3247	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3248	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3249	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3250	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3251	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3252	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3253	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3254	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3255	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3256	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3257	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3258	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3259	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3260	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3261	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3262	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3263	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3264	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3265	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3266	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3267	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3268	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3269	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3270	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3271	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3272	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3273	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3274	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3275	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3276	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3277	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3278	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3279	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3280	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3281	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3282	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3283	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3284</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3285</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3286</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3287</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3288</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3289	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3290	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3291	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3292	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3293	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3294	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3295	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3296	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3297	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3298	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3299	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3300	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3301	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3302	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3303	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3304	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3305	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3306	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3307</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3308</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3309</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3310</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3311</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3312	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3313	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3314	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3315	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3316	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3317	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3318	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3319	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3320	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3321	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3322	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3323</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3324</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3325</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3326</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2020-8286
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3327</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
<tr><td>3328</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 17, 2022 06:43:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3329	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3330	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3331	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3332	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3333	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3334	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21

ID	Name	Level	Location	Detail	Datetime
3335	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3336	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2020-8286 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 17, 2022 06:43:21
3337	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 17, 2022 06:43:21
3338	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:36:49
3339	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 17, 2022 06:36:49
3340	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:36:49
3341	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 17, 2022 06:36:49
3342	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:36:48

ID	Name	Level	Location	Detail	Datetime
3343	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:36:48
3344	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:36:48
3345	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 17, 2022 06:36:48
3346	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 236 Items) Total : 0 Items	Feb 17, 2022 06:36:48
3347	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:36:29

ID	Name	Level	Location	Detail	Datetime
3348	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:36:29
3349	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:36:29
3350	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 17, 2022 06:36:29
3351	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-kkvk9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2018-12886 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-10029 • CVE-2020-27618 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:32
3352	Container.Scan.Report	Info	**Container** : fluentbit-gke-tm92t **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:30
3353	Container.Scan.Report	Info	**Container** : event-exporter-gke-5479fd58c8-dktkd **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:29
3354	Container.Scan.Report	Critical	**Container** : pdcsi-node-4fhgs **Node** : gke-cluster-1-default-pool-d051acb1-tztv	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2018-12886 • ..... • (Total : 21 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 10 Items)	Feb 17, 2022 06:35:29
3355	Container.Scan.Report	Info	**Container** : fluentbit-gke-ljrgv **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:29

ID	Name	Level	Location	Detail	Datetime
3356	Container.Scan.Report	Critical	**Container** : pdcsi-node-mnzct **Node** : gke-cluster-1-default-pool-d051acb1-k0qs	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 21 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 10 Items)	Feb 17, 2022 06:35:29
3357	Host.Scan.Report	Critical	**Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : cos:89 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-5932 • CVE-2016-7543 • CVE-2019-20367 • ..... • (Total : 63 Items) Medium Vulnerabilities: • CVE-2018-15855 • CVE-2018-15861 • CVE-2018-15863 • ..... • (Total : 83 Items)	Feb 17, 2022 06:35:26
3358	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:35:26
3359	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:35:26
3360	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:35:26
3361	Container.Scan.Report	Info	**Container** : l7-default-backend-69fb9fd9f9-7fdjj **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:26
3362	Container.Scan.Report	Info	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-r9l9 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:26
3363	Container.Scan.Report	Info	**Container** : gke-metrics-agent-mrlvl **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:26

ID	Name	Level	Location	Detail	Datetime
3364	Container.Scan.Report	Info	**Container** : fluentbit-gke-tm92t **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:26
3365	Container.Scan.Report	Info	**Container** : pdcsi-node-8sfmp **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:26
3366	Container.Scan.Report	Info	**Container** : pdcsi-node-4fhgs **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:26
3367	Container.Scan.Report	Info	**Container** : fluentbit-gke-zx587 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:26
3368	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-kkvk9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:26
3369	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:35:26
3370	Container.Scan.Report	Info	**Container** : fluentbit-gke-tm92t **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:26
3371	Container.Scan.Report	Critical	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-k0qs **Node** : gke-cluster-1-default-pool-d051acb1-k0qs	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:22
3372	Container.Scan.Report	Info	**Container** : konnectivity-agent-autoscaler-5c49cb58bb-zv88w **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:22

ID	Name	Level	Location	Detail	Datetime
3373	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3374	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3375	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3376	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3377</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3378</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3379</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3380</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3381	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3382	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3383	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3384	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3385</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3386</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3387</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3388</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3389	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3390	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3391	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3392	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3393</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3394</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3395</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3396</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3397	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3398	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3399	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3400	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3401	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3402	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3403	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3404	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3405	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3406</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3407</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3408</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3409</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3410</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3411</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3412</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3413</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3414	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3415	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3416	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3417	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3418	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3419</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3420</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3421</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3422</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3423</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3424</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3425</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3426</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3427</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3428</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3429</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3430</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3431</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3432</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3433</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3434</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3435	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3436	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3437	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3438	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3439</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3440</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3441</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3442</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3443</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3444</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3445</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3446</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3447	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3448	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3449	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3450	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3451</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3452</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3453</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3454</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3455</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3456</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3457</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3458</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3459</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3460</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3461</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3462</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3463	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3464	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3465	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3466	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3467</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3468</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3469</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3470</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3471</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3472</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3473</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3474</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3475	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3476	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3477	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3478	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3479</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3480</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3481</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3482</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3483</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3484</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3485</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3486</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3487	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3488	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3489	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3490	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3491	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3492	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3493	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3494	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3495	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3496</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3497</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3498</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3499</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3500</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3501</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3502</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3503</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3504</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3505	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3506	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3507	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3508	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3509</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3510</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3511</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3512</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3513	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3514	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3515	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3516	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3517	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3518	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3519	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3520	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3521	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3522</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3523</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3524</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3525</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3526	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3527	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3528	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3529	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3530</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3531</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3532</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3533</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3534	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3535	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3536	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3537	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3538</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3539</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3540</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3541</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3542</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3543</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3544</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3545</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3546</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3547</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3548</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3549</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3550</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3551</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3552</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3553</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3554</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3555</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3556</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3557</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3558</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3559</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3560</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3561</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3562</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3563</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3564</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3565</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3566	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3567	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3568	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3569	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3570</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3571</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3572</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3573</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3574</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3575</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3576</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3577</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3578	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3579	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3580	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3581	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3582</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3583</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3584</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3585</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3586</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3587</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3588</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3589</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3590</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3591	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3592	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3593	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3594	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3595</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3596</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3597</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3598</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3599</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3600</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3601</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3602</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3603</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3604</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3605</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3606</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3607</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3608</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3609</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3610</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3611	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3612	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3613	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3614	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3615</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3616</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3617</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3618</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3619	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3620	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3621	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3622	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3623</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3624</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3625</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3626</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3627	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3628	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3629	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3630	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3631	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3632	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3633	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3634	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3635	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3636	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3637	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3638	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3639</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3640</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3641</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3642</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3643</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3644</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3645</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3646</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3647	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3648	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3649	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3650	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3651</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3652</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3653</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3654</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3655</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3656</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3657</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3658</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3659</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3660</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3661</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3662</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3663	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3664	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3665	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3666	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3667</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3668</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3669</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3670</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3671</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3672</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3673</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3674</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3675</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3676</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3677</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3678</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3679</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3680</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3681</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3682</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3683</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3684</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3685</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3686</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3687</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3688</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3689</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3690</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3691</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3692</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3693</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3694</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3695</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3696	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3697	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3698	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3699	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3700</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3701</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3702</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3703</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3704</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3705</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3706</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3707</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3708	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3709	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3710	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3711	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3712	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3713	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3714	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3715	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3716	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3717	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3718	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3719	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3720	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3721</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3722</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3723</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3724</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3725</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3726</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3727</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3728</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3729</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3730</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3731</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3732</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3733	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3734	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3735	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3736	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3737</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3738</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3739</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3740</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3741</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3742</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3743</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3744</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3745	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3746	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3747	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3748	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3749	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3750	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3751	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3752	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3753</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3754</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3755</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3756</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3757</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3758</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3759</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3760</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3761</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3762</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3763</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3764</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3765	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3766	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3767	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3768	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3769</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3770</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3771</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3772</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3773</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3774</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3775</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3776</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2016-1252
• CVE-2020-27350
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3777</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3778</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3779</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
<tr><td>3780</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.602
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2016-1252</li><li>CVE-2020-27350</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 17, 2022 06:35:21</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3781	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3782	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3783	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3784	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21

ID	Name	Level	Location	Detail	Datetime
3785	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3786	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 410 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2016-1252 • CVE-2020-27350 • ..... • (Total : 242 Items) Total : 0 Items	Feb 17, 2022 06:35:21
3787	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3788	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 17, 2022 06:35:21
3789	Container.Scan.Report	Info	**Container** : metrics-server-v0.4.4-857776bc9c-bfhbp **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:19

ID	Name	Level	Location	Detail	Datetime
3790	Container.Scan.Report	Info	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-9mr2 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:19
3791	Container.Scan.Report	Info	**Container** : gke-metrics-agent-mrlvl **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:19
3792	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-6j2xk **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:19
3793	Container.Scan.Report	Info	**Container** : pdcsi-node-2vpps **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:18
3794	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-jb8v6 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:18
3795	Container.Scan.Report	Info	**Container** : fluentbit-gke-6nc87 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:18
3796	Container.Scan.Report	Info	**Container** : metrics-server-v0.4.4-857776bc9c-bfhbp **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:18
3797	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-ksdst **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:18
3798	Container.Scan.Report	Info	**Container** : gke-metrics-agent-4h522 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:18
3799	Container.Scan.Report	Critical	**Container** : redis-pod-7bbd468657-jzzv4 **Node** : gke-cluster-1-default-pool-d051acb1-tztv	**Base OS** : debian:11 **CVE DB Version** : 2.602 High Vulnerabilities • CVE-2020-16156 Medium Vulnerabilities : 0	Feb 17, 2022 06:35:18
3800	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-c9mrq **Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2018-12886 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:17
3801	Container.Scan.Report	Info	**Container** : redis-pod-7bbd468657-jzzv4 **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:15
3802	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-ksdst **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:15

ID	Name	Level	Location	Detail	Datetime
3803	Container.Scan.Report	Critical	**Container** : pdcsi-node-2vpps **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2019-15847 • ..... • (Total : 21 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 10 Items)	Feb 17, 2022 06:35:15
3804	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-c9mrq **Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2018-12886 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:14
3805	Container.Scan.Report	Info	**Container** : kube-dns-697dc8fc8b-kkvk9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:14
3806	Container.Scan.Report	Info	**Container** : gke-metrics-agent-r4jh9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:14
3807	Container.Scan.Report	Critical	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-9mr2 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:12
3808	Host.Scan.Report	Critical	**Node** : gke-cluster-1-default-pool-d051acb1-tztv	**Base OS** : cos:89 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-5932 • CVE-2016-7543 • CVE-2019-20367 • ..... • (Total : 63 Items) Medium Vulnerabilities: • CVE-2018-15863 • CVE-2018-15859 • CVE-2018-15862 • ..... • (Total : 83 Items)	Feb 17, 2022 06:35:11
3809	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-w74kn **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:10
3810	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:35:09

ID	Name	Level	Location	Detail	Datetime
3811	Container.Scan.Report	Critical	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-5z3m **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:09
3812	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:35:09
3813	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2020-1751 • CVE-2018-11237 • CVE-2018-19591 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-27350 • ..... • (Total : 18 Items) Total : 0 Items	Feb 17, 2022 06:35:09
3814	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 17, 2022 06:35:09
3815	Container.Scan.Report	Info	**Container** : fluentbit-gke-6nc87 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:05
3816	Container.Scan.Report	Critical	**Container** : pdcsi-node-8sfmp **Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2018-12886 • ..... • (Total : 21 Items) Medium Vulnerabilities: • CVE-2020-10029 • CVE-2020-27618 • CVE-2020-27618 • ..... • (Total : 10 Items)	Feb 17, 2022 06:35:05
3817	Container.Scan.Report	Info	**Container** : kube-dns-autoscaler-844c9d9448-f5jlz **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:05
3818	Container.Scan.Report	Info	**Container** : gke-metrics-agent-n7ttl **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:02
3819	Container.Scan.Report	Info	**Container** : pdcsi-node-9s9js **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:02

ID	Name	Level	Location	Detail	Datetime
3820	Container.Scan.Report	Info	**Container** : gke-metrics-agent-r4jh9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:02
3821	Container.Scan.Report	Info	**Container** : fluentbit-gke-zx587 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:02
3822	Platform.Scan.Report	Info	**Platform** : kubernetes: 1.21.6-gke.1500		Feb 17, 2022 06:35:01
3823	Container.Scan.Report	Info	**Container** : fluentbit-gke-ljrgv **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:01
3824	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-bhlfs **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:35:01
3825	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-w74kn **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:01
3826	Container.Scan.Report	Info	**Container** : fluentbit-gke-6nc87 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:01
3827	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-c9mrq **Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-10029 • CVE-2020-27618 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:35:01
3828	Container.Scan.Report	Info	**Container** : gke-metrics-agent-4h522 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:35:01
3829	Container.Scan.Report	Info	**Container** : event-exporter-gke-5479fd58c8-dktkd **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:01
3830	Container.Scan.Report	Info	**Container** : pdcsi-node-4fhgs **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:35:00
3831	Container.Scan.Report	Info	**Container** : pdcsi-node-2vpps **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:35:00
3832	Host.Scan.Report	Critical	**Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : cos:89 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2017-5932 • CVE-2016-7543 • CVE-2019-20367 • ..... • (Total : 63 Items) Medium Vulnerabilities: • CVE-2018-15861 • CVE-2018-15863 • CVE-2018-15854 • ..... • (Total : 83 Items)	Feb 17, 2022 06:35:00

ID	Name	Level	Location	Detail	Datetime
3833	Container.Scan.Report	Info	**Container** : pdcsi-node-mnzct **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:35:00
3834	Container.Scan.Report	Info	**Container** : kube-dns-autoscaler-844c9d9448-f5jlz **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:34:57
3835	Container.Scan.Report	Info	**Container** : fluentbit-gke-cfn4g **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:34:57
3836	Container.Scan.Report	Info	**Container** : fluentbit-gke-ljrgv **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:34:57
3837	Container.Scan.Report	Critical	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-r9l9 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 6 Items)	Feb 17, 2022 06:34:57
3838	Container.Scan.Report	Info	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-k0qs **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:57
3839	Container.Scan.Report	Info	**Container** : gke-metrics-agent-n7ttl **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:57
3840	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:34:56
3841	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 17, 2022 06:34:56
3842	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:34:56

ID	Name	Level	Location	Detail	Datetime
3843	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 17, 2022 06:34:56
3844	Container.Scan.Report	Critical	**Container** : pdcsi-node-9s9js **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-12886 • CVE-2019-15847 • CVE-2018-12886 • ..... • (Total : 21 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-10029 • ..... • (Total : 10 Items)	Feb 17, 2022 06:34:53
3845	Container.Scan.Report	Info	**Container** : pdcsi-node-8sfmp **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:34:53
3846	Container.Scan.Report	Info	**Container** : kube-dns-697dc8fc8b-c9mrq **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:34:53
3847	Container.Scan.Report	Info	**Container** : metrics-server-v0.4.4-857776bc9c-bfhbp **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:34:49
3848	Host.Scan.Report	Critical	**Node** : gke-cluster-1-default-pool-d051acb1-9mr2	**Base OS** : cos:89 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2016-7543 • CVE-2017-5932 • CVE-2019-20367 • ..... • (Total : 63 Items) Medium Vulnerabilities: • CVE-2018-15858 • CVE-2018-15859 • CVE-2018-15855 • ..... • (Total : 83 Items)	Feb 17, 2022 06:34:49
3849	Container.Scan.Report	Critical	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-tztv **Node** : gke-cluster-1-default-pool-d051acb1-tztv	**Base OS** : debian:10 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2018-12886 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:34:49
3850	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-6j2xk **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:45
3851	Container.Scan.Report	Info	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-tztv **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:34:45

ID	Name	Level	Location	Detail	Datetime
3852	Host.Scan.Report	Critical	**Node** : gke-cluster-1-default-pool-d051acb1-k0qs	**Base OS** : cos:89 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-5932 • CVE-2016-7543 • CVE-2019-20367 • ..... • (Total : 63 Items) Medium Vulnerabilities: • CVE-2018-15862 • CVE-2018-15859 • CVE-2018-15854 • ..... • (Total : 83 Items)	Feb 17, 2022 06:34:45
3853	Container.Scan.Report	Info	**Container** : fluentbit-gke-cfn4g **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:34:38
3854	Container.Scan.Report	Info	**Container** : event-exporter-gke-5479fd58c8-dktkd **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:38
3855	Container.Scan.Report	Info	**Container** : kube-proxy-gke-cluster-1-default-pool-d051acb1-5z3m **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:34:38
3856	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-bhlfs **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:34:38
3857	Container.Scan.Report	Info	**Container** : konnectivity-agent-autoscaler-5c49cb58bb-zv88w **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:38
3858	Container.Scan.Report	Info	**Container** : gke-metrics-agent-p4zv8 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:34:38
3859	Container.Scan.Report	Info	**Container** : fluentbit-gke-cfn4g **Node** : gke-cluster-1-default-pool-d051acb1-tztv		Feb 17, 2022 06:34:38
3860	Container.Scan.Report	Info	**Container** : pdcsi-node-mnzct **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:38
3861	Container.Scan.Report	Info	**Container** : fluentbit-gke-zx587 **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:34:37
3862	Container.Scan.Report	Info	**Container** : kube-dns-697dc8fc8b-c9mrq **Node** : gke-cluster-1-default-pool-d051acb1-r9l9		Feb 17, 2022 06:34:37
3863	Container.Scan.Report	Critical	**Container** : kube-dns-697dc8fc8b-kkvk9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m	**Base OS** : debian:10 **CVE DB Version** : 2.602 High Vulnerabilities: • CVE-2019-15847 • CVE-2018-12886 • CVE-2019-15847 • ..... • (Total : 18 Items) Medium Vulnerabilities: • CVE-2020-27618 • CVE-2020-10029 • CVE-2020-27618 • ..... • (Total : 6 Items)	Feb 17, 2022 06:34:37

ID	Name	Level	Location	Detail	Datetime
3864	Container.Scan.Report	Info	**Container** : l7-default-backend-69fb9fd9f9-7fdjj **Node** : gke-cluster-1-default-pool-d051acb1-k0qs		Feb 17, 2022 06:34:35
3865	Container.Scan.Report	Info	**Container** : konnectivity-agent-86678fb5f5-jb8v6 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:34:35
3866	Container.Scan.Report	Info	**Container** : kube-dns-697dc8fc8b-kkvk9 **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:34:35
3867	Container.Scan.Report	Info	**Container** : pdcsi-node-9s9js **Node** : gke-cluster-1-default-pool-d051acb1-5z3m		Feb 17, 2022 06:34:35
3868	Container.Scan.Report	Info	**Container** : gke-metrics-agent-p4zv8 **Node** : gke-cluster-1-default-pool-d051acb1-9mr2		Feb 17, 2022 06:34:35
3869	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3870	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3871	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3872	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47

ID	Name	Level	Location	Detail	Datetime
3873	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3874	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3875	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3876	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3877	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3878	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3879</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2018-16890
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:50:47</td></tr>
<tr><td>3880</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 16, 2022 19:50:47</td></tr>
<tr><td>3881</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 16, 2022 19:50:47</td></tr>
<tr><td>3882</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2018-16890
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:50:47</td></tr>
<tr><td>3883</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 169 files have setgid mode
• I.4.8 WARN - Total 11 files have setuid mode</td><td>Feb 16, 2022 19:50:47</td></tr>
<tr><td>3884</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/exploit_1_21:latest</td><td>Base OS : kali:2018.4
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-12900
• CVE-2019-12900
• CVE-2018-16890
• .....
• (Total : 348 Items)</td><td>• CVE-2020-3810
• CVE-2020-3810
• CVE-2020-3810
• .....
• (Total : 234 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:50:47</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
3885	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3886	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3887	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3888	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3889	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3890	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47

ID	Name	Level	Location	Detail	Datetime
3891	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	**Base OS** : kali:2018.4 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-12900 • CVE-2019-12900 • CVE-2018-16890 • ..... • (Total : 348 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 234 Items) Total : 0 Items	Feb 16, 2022 19:50:47
3892	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3893	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3894	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/exploit_1_21:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 169 files have setgid mode • I.4.8 WARN - Total 11 files have setuid mode	Feb 16, 2022 19:50:47
3895	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3896	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3897	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3898	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3899	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3900	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09

ID	Name	Level	Location	Detail	Datetime
3901	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3902	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3903	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3904	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3905	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3906	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3907	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3908	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3909	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3910	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3911	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3912	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3913	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3914	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3915	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09

ID	Name	Level	Location	Detail	Datetime
3916	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3917	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3918	Registry.Scan.Report	Info	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	Total : 0 Items	Feb 16, 2022 19:45:09
3919	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3920	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/hello-world:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images	Feb 16, 2022 19:45:09
3921	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3922	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3923	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3924	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3925	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3926	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3927	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3928	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3929	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3930	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3931	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3932	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3933	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3934	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3935	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3936	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3937	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3938	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3939	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3940	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3941	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3942	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3943	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3944	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3945	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3946	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3947	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3948	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3949	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3950	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3951	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3952	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3953	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3954	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3955	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3956	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3957	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3958	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3959	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3960	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3961	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3962	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3963	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3964	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3965	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3966	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3967	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3968	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key contains privatekey • I.4.10 WARN - File /build/insecure_key.ppk contains privatekey • I.4.8 WARN - Total 14 files have setgid mode • I.4.8 WARN - Total 14 files have setuid mode	Feb 16, 2022 19:45:08
3969	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3970	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08
3971	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/dns_client2:latest	**Base OS** : ubuntu:14.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-3462 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 394 Items) Medium Vulnerabilities: • CVE-2016-1252 • CVE-2020-3810 • CVE-2020-27350 • ..... • (Total : 236 Items) Total : 0 Items	Feb 16, 2022 19:45:08

ID	Name	Level	Location	Detail	Datetime
3972	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3973	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3974	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3975	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3976	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3977	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3978	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49

ID	Name	Level	Location	Detail	Datetime
3979	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3980	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3981	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3982	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3983	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3984	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3985	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49

ID	Name	Level	Location	Detail	Datetime
3986	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3987	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3988	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3989	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3990	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3991	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3992	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49

ID	Name	Level	Location	Detail	Datetime
3993	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3994	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3995	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49
3996	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 279 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:49
3997	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/api_server:latest	**Base OS** : debian:9 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2017-12613 • CVE-2019-3462 • CVE-2019-3462 • ..... • (Total : 1635 Items) Medium Vulnerabilities: • CVE-2020-27350 • CVE-2020-3810 • CVE-2020-3810 • ..... • (Total : 1494 Items) Total : 0 Items	Feb 16, 2022 19:44:49

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>3998</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>3999</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4000</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4001</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>4002</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4003</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4004</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4005</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>4006</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4007</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4008</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td><ul><li>I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles</li><li>I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey</li><li>I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey</li><li>I.4.8 WARN - Total 17 files have setgid mode</li><li>I.4.8 WARN - Total 13 files have setuid mode</li></ul></td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4009</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td><ul><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>CVE-2019-3462</li><li>.....</li><li>(Total : 410 Items)</li></ul></td><td><ul><li>CVE-2020-3810</li><li>CVE-2020-27350</li><li>CVE-2016-1252</li><li>.....</li><li>(Total : 242 Items)</li></ul></td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
4010	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 16, 2022 19:44:07
4011	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 16, 2022 19:44:07
4012	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 16, 2022 19:44:07
4013	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/node:latest	• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey • I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey • I.4.8 WARN - Total 17 files have setgid mode • I.4.8 WARN - Total 13 files have setuid mode	Feb 16, 2022 19:44:07

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>4014</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4015</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4016</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4017</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
</table>

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>4018</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4019</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4020</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>• I.4.9 WARN - Ensure that COPY is used instead of ADD in Dockerfiles
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssh/ssh_host_rsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_dsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ecdsa_key contains privatekey
• I.4.10 WARN - File /etc/ssh/ssh_host_ed25519_key contains privatekey
• I.4.8 WARN - Total 17 files have setgid mode
• I.4.8 WARN - Total 13 files have setuid mode</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4021</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/node:latest</td><td>Base OS : ubuntu:14.04
CVE DB Version : 2.601
<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-3462
• CVE-2019-3462
• CVE-2019-3462
• .....
• (Total : 410 Items)</td><td>• CVE-2020-3810
• CVE-2020-27350
• CVE-2016-1252
• .....
• (Total : 242 Items)</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:07</td></tr>
<tr><td>4022</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 16, 2022 19:44:03</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
4023	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4024	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4025	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4026	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4027	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4028	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03

ID	Name	Level	Location	Detail	Datetime
4029	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4030	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4031	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4032	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4033	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4034	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03

ID	Name	Level	Location	Detail	Datetime
4035	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4036	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4037	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4038	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03
4039	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4040	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:44:03

<table>
<tr><th>ID</th><th>Name</th><th>Level</th><th>Location</th><th>Detail</th><th>Datetime</th></tr>
<tr><td>4041</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-9511
• CVE-2017-7529
• CVE-2021-23017</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:03</td></tr>
<tr><td>4042</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 16, 2022 19:44:03</td></tr>
<tr><td>4043</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-9511
• CVE-2017-7529
• CVE-2021-23017</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:03</td></tr>
<tr><td>4044</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-9511
• CVE-2017-7529
• CVE-2021-23017</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:03</td></tr>
<tr><td>4045</td><td>Compliance.Image.Violation</td><td>Warning</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>• I.4.1 WARN - Ensure a user for the container has been created
• I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images
• I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey
• I.4.8 WARN - Total 18 files have setgid mode
• I.4.8 WARN - Total 10 files have setuid mode</td><td>Feb 16, 2022 19:44:03</td></tr>
<tr><td>4046</td><td>Registry.Scan.Report</td><td>Critical</td><td>Registry : https://registry.hub.docker.com/
Image : nvbeta/nginx:latest</td><td>Base OS : debian:8
CVE DB Version : 2.601<table><tr><th>High Vulnerabilities</th><th>Medium Vulnerabilities</th></tr><tr><td>• CVE-2019-9511
• CVE-2017-7529
• CVE-2021-23017</td><td>• CVE-2018-16845</td></tr></table>Total : 0 Items</td><td>Feb 16, 2022 19:44:03</td></tr>
</table>

ID	Name	Level	Location	Detail	Datetime
4047	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:44:03
4048	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4049	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4050	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4051	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4052	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52

ID	Name	Level	Location	Detail	Datetime
4053	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4054	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4055	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4056	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4057	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4058	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4059	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52

ID	Name	Level	Location	Detail	Datetime
4060	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4061	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4062	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4063	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4064	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4065	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4066	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52

ID	Name	Level	Location	Detail	Datetime
4067	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4068	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4069	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.8 WARN - Total 7 files have setgid mode • I.4.8 WARN - Total 8 files have setuid mode	Feb 16, 2022 19:43:52
4070	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4071	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52
4072	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/iodine:latest	**Base OS** : ubuntu:18.04 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2018-11236 • CVE-2018-19591 • CVE-2018-11237 • ..... • (Total : 15 Items) Medium Vulnerabilities: • CVE-2020-3810 • CVE-2020-27350 • CVE-2020-3810 • ..... • (Total : 18 Items) Total : 0 Items	Feb 16, 2022 19:43:52

ID	Name	Level	Location	Detail	Datetime
4073	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4074	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4075	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4076	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4077	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4078	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41

ID	Name	Level	Location	Detail	Datetime
4079	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4080	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4081	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4082	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4083	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4084	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41

ID	Name	Level	Location	Detail	Datetime
4085	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4086	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4087	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4088	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4089	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4090	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41

ID	Name	Level	Location	Detail	Datetime
4091	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4092	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4093	Registry.Scan.Report	Critical	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	**Base OS** : debian:8 **CVE DB Version** : 2.601 High Vulnerabilities: • CVE-2019-9511 • CVE-2017-7529 • CVE-2021-23017 Medium Vulnerabilities: • CVE-2018-16845 Total : 0 Items	Feb 16, 2022 19:43:41
4094	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4095	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41
4096	Compliance.Image.Violation	Warning	**Registry** : https://registry.hub.docker.com/ **Image** : nvbeta/swarm_nginx:latest	• I.4.1 WARN - Ensure a user for the container has been created • I.4.6 WARN - Ensure that HEALTHCHECK instructions have been added to container images • I.4.10 WARN - File /etc/ssl/private/ssl-cert-snakeoil.key contains privatekey • I.4.8 WARN - Total 18 files have setgid mode • I.4.8 WARN - Total 10 files have setuid mode	Feb 16, 2022 19:43:41