

# Quay Registry Report – Critical vulnerabilities in 014014-cdmdip-dqt

## sparta\_kb\_source – Version 1.1.083-129

014014-cdmdip-dqt/sparta\_kb\_source

ed1d2c600310

Quay Security Scanner has detected **202** vulnerabilities.  
Patches are available for **8** vulnerabilities.

- 2 Critical-level vulnerabilities.
- 7 High-level vulnerabilities.
- 28 Medium-level vulnerabilities.
- 21 Low-level vulnerabilities.
- 141 Negligible-level vulnerabilities.
- 3 Unknown-level vulnerabilities.

Vulnerabilities

Filter Vulnerabilities... ☐ Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER																								
▼ CVE-2019-19814	Critical	linux	4.19.132-1	(None)	<div>RUN</div> apt-get update && apt-get install gcc -y && ..																								
<div>SEVERITY NOTE</div> <p>Note that this vulnerability was originally given a CVSSv2 score of <b>9.3</b> by NVD but was subsequently reclassified as <b>Critical</b> by debian</p> <div>VECTORS</div> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td><b>Network</b></td><td>Low</td><td><b>None</b></td><td><b>Complete</b></td><td><b>Complete</b></td><td><b>Complete</b></td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <div>DESCRIPTION</div> <p>In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.</p>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								
▼ CVE-2019-19816	Critical	linux	4.19.132-1	(None)	<div>RUN</div> apt-get update && apt-get install gcc -y && ..																								
<div>SEVERITY NOTE</div> <p>Note that this vulnerability was originally given a CVSSv2 score of <b>9.3</b> by NVD but was subsequently reclassified as <b>Critical</b> by debian</p> <div>VECTORS</div> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td><b>Network</b></td><td>Low</td><td><b>None</b></td><td><b>Complete</b></td><td><b>Complete</b></td><td><b>Complete</b></td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <div>DESCRIPTION</div> <p>In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.</p>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								

## sparta\_wl\_screening – Version 1.0.60-102

014014-cdmip-dqt/sparta-wl-screening

fb0cb43ac7d9

Quay Security Scanner has detected **280** vulnerabilities.  
Patches are available for **31** vulnerabilities.

- 2 Critical-level vulnerabilities.
- 10 High-level vulnerabilities.
- 43 Medium-level vulnerabilities.
- 33 Low-level vulnerabilities.
- 178 Negligible-level vulnerabilities.
- 14 Unknown-level vulnerabilities.

Vulnerabilities

Filter Vulnerabilities... ☐ Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER																								
▼ CVE-2019-19814	Critical	linux	4.19.118-2+deb10u1	(None)	<b>RUN</b> apt install build-essential libbig-dev libnc...																								
<p><b>SEVERITY NOTE</b> Note that this vulnerability was originally given a CVSSv2 score of <b>9.3</b> by NVD but was subsequently reclassified as <b>Critical</b> by debian</p> <p><b>VECTORS</b></p> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td><b>Network</b></td><td>Low</td><td><b>None</b></td><td><b>Complete</b></td><td><b>Complete</b></td><td><b>Complete</b></td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <p><b>DESCRIPTION</b> In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.</p>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								
▼ CVE-2019-19816	Critical	linux	4.19.118-2+deb10u1	(None)	<b>RUN</b> apt install build-essential libbig-dev libnc...																								
<p><b>SEVERITY NOTE</b> Note that this vulnerability was originally given a CVSSv2 score of <b>9.3</b> by NVD but was subsequently reclassified as <b>Critical</b> by debian</p> <p><b>VECTORS</b></p> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td><b>Network</b></td><td>Low</td><td><b>None</b></td><td><b>Complete</b></td><td><b>Complete</b></td><td><b>Complete</b></td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <p><b>DESCRIPTION</b> In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.</p>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
<b>Network</b>	Low	<b>None</b>	<b>Complete</b>	<b>Complete</b>	<b>Complete</b>																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								

## sparta-wl-index – Version 1.0.51-72

014014-cdmip-dqt/sparta-wl-index

cd42731f650a

Quay Security Scanner has detected **280** vulnerabilities.

Patches are available for **31** vulnerabilities.

2 Critical-level vulnerabilities.

10 High-level vulnerabilities.

43 Medium-level vulnerabilities.

33 Low-level vulnerabilities.

178 Negligible-level vulnerabilities.

14 Unknown-level vulnerabilities.

Vulnerabilities

Filter Vulnerabilities... ☐ Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER																								
▼ CVE-2019-19814	Critical	linux	4.19.118-2+deb10u1	(None)	<div>RUN</div> apt install build-essential cifs-utils libnc...																								
<div>SEVERITY NOTE</div> <div>Note that this vulnerability was originally given a CVSSv2 score of 9.3 by NVD but was subsequently reclassified as Critical by debian</div> <div>VECTORS</div> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td>Network</td><td>Low</td><td>None</td><td>Complete</td><td>Complete</td><td>Complete</td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <div>DESCRIPTION</div> <div>In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.</div>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Network	Low	None	Complete	Complete	Complete	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
Network	Low	None	Complete	Complete	Complete																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								
▼ CVE-2019-19816	Critical	linux	4.19.118-2+deb10u1	(None)	<div>RUN</div> apt install build-essential cifs-utils libnc...																								
<div>SEVERITY NOTE</div> <div>Note that this vulnerability was originally given a CVSSv2 score of 9.3 by NVD but was subsequently reclassified as Critical by debian</div> <div>VECTORS</div> <table><thead><tr><th>Access Vector</th><th>Access Complexity</th><th>Authentication</th><th>Confidentiality Impact</th><th>Integrity Impact</th><th>Availability Impact</th></tr></thead><tbody><tr><td>Network</td><td>Low</td><td>None</td><td>Complete</td><td>Complete</td><td>Complete</td></tr><tr><td>Adjacent Network</td><td>Medium</td><td>Single</td><td>Partial</td><td>Partial</td><td>Partial</td></tr><tr><td>Local</td><td>High</td><td>Multiple</td><td>None</td><td>None</td><td>None</td></tr></tbody></table> <div>DESCRIPTION</div> <div>In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.</div>						Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Network	Low	None	Complete	Complete	Complete	Adjacent Network	Medium	Single	Partial	Partial	Partial	Local	High	Multiple	None	None	None
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact																								
Network	Low	None	Complete	Complete	Complete																								
Adjacent Network	Medium	Single	Partial	Partial	Partial																								
Local	High	Multiple	None	None	None																								

3