



# CVE-2022-1652

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-1652
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-02 14:15:00 UTC
<b>Updated</b>	2023-03-01 20:16:00 UTC
<b>Description</b>	Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free fl

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

## References

Reference	Source	Link
-----------	--------	------

1832397 – (CVE-2020-10135) CVE-2020-10135 kernel: bluetooth: BR/EDR Bluetooth Impersonation Attacks (BIAS)	MISC	<a href="#">bugzilla.re</a>
VU#647177 - Bluetooth devices supporting BR/EDR are vulnerable to impersonation attacks	MISC	<a href="#">kb.cert.or</a>
CVE-2022-1652 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.n</a>
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	<a href="#">www.debi</a>
2084458 – (CVE-2022-1652) CVE-2022-1652 kernel: A concurrency use-after-free in bad_flp_intr	MISC	<a href="#">bugzilla.re</a>
Search	MISC	<a href="#">francozap</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159969</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9557)
<a href="#">159974</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9583)
<a href="#">159975</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9582)
<a href="#">159979</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9591)
<a href="#">159982</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9590)
<a href="#">180605</a> Debian Security Update for linux (DSA 5173-1)
<a href="#">180608</a> Debian Security Update for linux (CVE-2022-1652)
<a href="#">198868</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5529-1)
<a href="#">198880</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5544-1)
<a href="#">198891</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5560-1)
<a href="#">198894</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5566-1)
<a href="#">198895</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5562-1)
<a href="#">198897</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5564-1)
<a href="#">198911</a> Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5582-1)
<a href="#">377117</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)
<a href="#">390262</a> Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0019)
<a href="#">672016</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2273)
<a href="#">672017</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2244)
<a href="#">672037</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2257)

<a href="#">672218</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2619)
<a href="#">752228</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2078-1)
<a href="#">752231</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)
<a href="#">752234</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2080-1)
<a href="#">752237</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2083-1)
<a href="#">752240</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2103-1)
<a href="#">752242</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2104-1)
<a href="#">752250</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2111-1)
<a href="#">752254</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2116-1)
<a href="#">752370</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
<a href="#">753114</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:3407-1)
<a href="#">753148</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)
<a href="#">753192</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 28 for SLE 15) (SUSE-SU-2022:3360-1)
<a href="#">753254</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP2) (SUSE-SU-2022:3476-1)
<a href="#">753296</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2177-1)
<a href="#">753314</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 25 for SLE 15 SP2) (SUSE-SU-2022:3445-1)
<a href="#">753335</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:3370-1)
<a href="#">753368</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2079-1)
<a href="#">753376</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:3368-1)
<a href="#">753379</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15) (SUSE-SU-2022:3424-1)
<a href="#">753395</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:3409-1)
<a href="#">753424</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP1) (SUSE-SU-2022:3359-1)
<a href="#">753458</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP3) (SUSE-SU-2022:3433-1)
<a href="#">753480</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 15 SP3) (SUSE-SU-2022:3464-1)
<a href="#">753703</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
<a href="#">753707</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
<a href="#">753727</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
<a href="#">902151</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9869)

[902156](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9878)

[902619](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9878-1)

[902689](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9869-1)

[906120](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9869-2)

[906440](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9878-2)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)