



# CVE-2021-3347

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

## Summary

<b>CVE</b>	CVE-2021-3347
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-29 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:37:00 UTC
<b>Description</b>	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault han

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	T
oss-security - Re: Linux Kernel: local priv escalation via futexes	MISC	<a href="http://www.openwall.com">www.openwall.com</a>	M
[SECURITY] [DLA 2557-1] linux-4.19 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	M
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="http://git.kernel.org">git.kernel.org</a>	M
[SECURITY] [DLA 2586-1] linux security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	M
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="http://git.kernel.org">git.kernel.org</a>	M

kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
CVE-2021-3347 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	T
oss-security - Linux Kernel: local priv escalation via futexes	MISC	<a href="https://www.openwall.com">www.openwall.com</a>	M
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
oss-security - Re: Linux Kernel: local priv escalation via futexes	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	M
Debian -- Security Information -- DSA-4843-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	T
[SECURITY] Fedora 32 Update: kernel-5.10.12-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	M
oss-security - Re: Linux Kernel: local priv escalation via futexes	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	E
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
[SECURITY] Fedora 32 Update: kernel-5.10.12-100.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 33 Update: kernel-5.10.12-200.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
oss-security - Re: Linux Kernel: local priv escalation via futexes	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	M
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
[SECURITY] Fedora 33 Update: kernel-5.10.12-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	M
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	M
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	c
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	c

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- 159144 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1093)
- 159258 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-2314)
- 159373 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-9434)
- 174805 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 0 for SLE 15 SP2) (SUSE-SU-2021:0849-1)
- 174807 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 7 for SLE 15 SP2) (SUSE-SU-2021:0842-1)
- 174808 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 36 for SLE 12 SP2) (SUSE-SU-2021:0870-1)
- 174809 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 0 for SLE 15 SP2) (SUSE-SU-2021:0849-1)
- 174810 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 19 for SLE 15 SP1) (SUSE-SU-2021:0853-1)
- 174811 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 9 for SLE 15 SP2) (SUSE-SU-2021:0840-1)
- 174812 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 13 for SLE 15 SP1) (SUSE-SU-2021:0859-1)
- 174813 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 5 for SLE 12 SP5) (SUSE-SU-2021:0818-1)

<a href="#">174817</a> SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 8 for SLE 15 SP2) (SUSE-SU-2021:0841-1)
<a href="#">174818</a> SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 14 for SLE 12 SP5) (SUSE-SU-2021:0809-1)
<a href="#">174819</a> SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 18 for SLE 15) (SUSE-SU-2021:0868-1)
<a href="#">179735</a> Debian Security Update for linux (CVE-2021-3347)
<a href="#">198297</a> Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4878-1)
<a href="#">198304</a> Ubuntu Security Notification for Linux-oem-5.10 Vulnerabilities (USN-4884-1)
<a href="#">198324</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4907-1)
<a href="#">198326</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4910-1)
<a href="#">239202</a> Red Hat Update for kernel (RHSA-2021:1093)
<a href="#">239204</a> Red Hat Update for kernel-rt (RHSA-2021:1081)
<a href="#">239236</a> Red Hat Update for kpatch-patch (RHSA-2021:1295)
<a href="#">239238</a> Red Hat Update for kernel (RHSA-2021:1272)
<a href="#">239253</a> Red Hat Update for kernel-alt (RHSA-2021:1379)
<a href="#">239271</a> Red Hat Update for kernel-alt (RHSA-2021:1379)
<a href="#">239349</a> Red Hat Update for kernel (RHSA-2021:2106)
<a href="#">239351</a> Red Hat Update for kpatch-patch (RHSA-2021:2099)
<a href="#">239403</a> Red Hat Update for kernel (RHSA-2021:2314)
<a href="#">239413</a> Red Hat Update for kpatch-patch (RHSA-2021:2285)
<a href="#">239452</a> Red Hat Update for kernel-rt (RHSA-2021:2316)
<a href="#">239455</a> Red Hat Update for kernel-rt (RHSA-2021:1279)
<a href="#">257092</a> CentOS Security Update for kernel (CESA-2021:2314)
<a href="#">352327</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-041
<a href="#">352328</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-040
<a href="#">352329</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-039
<a href="#">353131</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-020
<a href="#">377055</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2021:0027)
<a href="#">610357</a> Google Android Devices August 2021 Security Patch Missing
<a href="#">6140187</a> AWS Bottlerocket Security Update for kernel (GHSA-mq26-2rrr-55xf)

670345 EulerOS Security Update for kernel (EulerOS-SA-2021-1879)
670375 EulerOS Security Update for kernel (EulerOS-SA-2021-1950)
670396 EulerOS Security Update for kernel (EulerOS-SA-2021-1929)
670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)
670744 EulerOS Security Update for kernel (EulerOS-SA-2021-2502)
670936 EulerOS Security Update for kernel (EulerOS-SA-2021-1929)
671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)
730228 McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-3611)
750373 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0241-1)
900098 CBL-Mariner Linux Security Update for kernel 5.4.91
902971 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3837)
940387 AlmaLinux Security Update for kernel (ALSA-2021:1093)

© [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](#)**