



CVE-2020-12655

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

Summary

CVE	CVE-2020-12655
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-05 06:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	An issue was discovered in xfs_agf_verify in fs/xfs/libxfs/xfs_alloc.c in the Linux kernel through 5.6.10. Attackers may trigger

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Ta
[SECURITY] [DLA 2420-2] linux regression update	MLIST	lists.debian.org	
[SECURITY] Fedora 30 Update: kernel-5.6.13-100.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2323-1] linux-4.19 new package	MLIST	lists.debian.org	
USN-4483-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] Fedora 30 Update: kernel-5.6.13-100.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
xfs: add agf freeblocks verify in xfs_agf_verify · torvalds/linux@d0c7fea · GitHub	MISC	github.com	Pa
May 2020 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Re: [PATCH v3] xfs: add agf freeblocks verify in xfs_agf_verify - Darrick J. Wong		lore.kernel.org	
[SECURITY] Fedora 32 Update: kernel-5.6.13-300.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 31 Update: kernel-5.6.13-200.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: kernel-5.6.13-300.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2420-1] linux security update	MLIST	lists.debian.org	
[SECURITY] Fedora 31 Update: kernel-5.6.13-200.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

USN-4465-1: linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
USN-4485-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Pa
Re: [PATCH v3] xfs: add agf freeblocks verify in xfs_agf_verify - Darrick J. Wong	MISC	lore.kernel.org	Ve
[security-announce] openSUSE-SU-2020:0801-1: important: Security update	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)
- [160190](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9969)
- [352342](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-026
- [352343](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-025
- [751451](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
- [900078](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903388](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1928)
- [905781](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1928-1)
- [940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

© [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