



# CVE-2021-28971

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-28971
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-22 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:32:00 UTC
<b>Description</b>	In intel_pmu_drain_pebs_nhm in arch/x86/events/intel/ds.c in the Linux kernel through 5.11.8 on some Haswell CPUs, user

## Risk And Classification

**Problem Types:** CWE-755

## 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>	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>	34	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff 500f</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff 500f Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff A250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff A250 Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller Firmware</a>	-	All	All	All

## References

Reference	Source	Link	T
[SECURITY] Fedora 34 Update: kernel-5.11.9-300.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 32 Update: kernel-5.11.10-100.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 2689-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	

[SECURITY] Fedora 34 Update: kernel-5.11.9-300.fc34 - 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>
[SECURITY] Fedora 33 Update: kernel-5.11.9-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 33 Update: kernel-5.11.9-200.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
March 2021 Linux Kernel 5.11.8 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[SECURITY] Fedora 32 Update: kernel-5.11.10-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159177](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9220)

[159178](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9221)

[159179](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9222)

[159180](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9223)

[159492](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)

[174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)

[174897](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)

[174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

[174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

[178679](#) Debian Security Update for linux-4.19 (DLA 2690-1)

[178680](#) Debian Security Update for linux (DLA 2689-1)

[180423](#) Debian Security Update for linux (CVE-2021-28971)

[198365](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)

[198398](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4979-1)

[198401](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4982-1)

[198403](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4984-1)

[239816](#) Red Hat Update for kernel security (RHSA-2021:4356)

<a href="#">239879</a> Red Hat Update for kernel-rt (RHSA-2021:4140)
<a href="#">281407</a> Fedora Security Update for kernel (FEDORA-2021-9503ffad9)
<a href="#">281424</a> Fedora Security Update for kernel (FEDORA-2021-68b0dd2373)
<a href="#">281425</a> Fedora Security Update for kernel (FEDORA-2021-e636ce53df)
<a href="#">352366</a> Amazon Linux Security Advisory for kernel: ALAS-2021-1503
<a href="#">353100</a> Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
<a href="#">353101</a> Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
<a href="#">353102</a> Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
<a href="#">353149</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-002
<a href="#">6140145</a> AWS Bottlerocket Security Update for kernel (GHSA-5q9c-rrw2-47f6)
<a href="#">670449</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2051)
<a href="#">750004</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
<a href="#">750006</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
<a href="#">750015</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
<a href="#">750199</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
<a href="#">750276</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)
<a href="#">750650</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
<a href="#">750652</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
<a href="#">750762</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
<a href="#">750766</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
<a href="#">900100</a> CBL-Mariner Linux Security Update for kernel 5.10.52.1
<a href="#">900305</a> CBL-Mariner Linux Security Update for kernel 5.10.57.1
<a href="#">900320</a> CBL-Mariner Linux Security Update for kernel 5.10.60.1
<a href="#">901522</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6542-1)
<a href="#">903612</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4010)
<a href="#">906045</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4010-1)
<a href="#">940265</a> AlmaLinux Security Update for kernel (ALSA-2021:4356)

© [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](#)**