



CVE-2020-36158

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-36158 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-01-05 05:15:00 UTC |
| Updated | 2023-11-07 03:22:00 UTC |
| Description | mwifiex_cmd_802_11_ad_hoc_start in drivers/net/wireless/marvell/mwifiex/join.c in the Linux kernel through 5.10.4 might a |

Risk And Classification

Problem Types: CWE-120

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 | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Hardware | Netapp | Solidfire Baseboard Management Controller | - | All | All | All |
| Operating System | Netapp | Solidfire Baseboard Management Controller Firmware | - | All | All | All |

References

| Reference | Source | Link |
|---|--------|---|
| [1/1] mwifiex: Fix possible buffer overflows in mwifiex_cmd_802_11_ad_hoc_start - Patchwork | | patchwork.kernel.org |
| [SECURITY] Fedora 33 Update: kernel-5.10.6-200.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] [DLA 2557-1] linux-4.19 security update | MLIST | lists.debian.org |
| [PATCH 1/1] mwifiex: Fix possible buffer overflows in mwifiex_cmd_802_11_ad_hoc_start - Xiaohui Zhang | MISC | lore.kernel.org |
| [SECURITY] [DLA 2586-1] linux security update | MLIST | lists.debian.org |

| | | |
|---|---------|--|
| [SECURITY] Fedora 33 Update: kernel-5.10.6-200.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [PATCH 1/1] mwifiex: Fix possible buffer overflows in mwifiex_cmd_802_11_ad_hoc_start - Xiaohui Zhang | | lore.kernel.org |
| Debian -- Security Information -- DSA-4843-1 linux | DEBIAN | www.debian.org |
| mwifiex: Fix possible buffer overflows in mwifiex_cmd_802_11_ad_hoc_start · torvalds/linux@5c455c5 · GitHub | MISC | github.com |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org |
| [1/1] mwifiex: Fix possible buffer overflows in mwifiex_cmd_802_11_ad_hoc_start - Patchwork | MISC | patchwork.kernel.org |
| CVE-2020-36158 Linux Kernel Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356) |
| 198295 Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-lts-xenial, Linux-raspi2, (USN-4876-1) |
| 198296 Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, (USN-4877-1) |
| 198297 Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4878-1) |
| 198298 Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-gcp, Linux-hwe-5.8, Linux-kvm, (USN-4879-1) |
| 198328 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4912-1) |
| 239816 Red Hat Update for kernel security (RHSA-2021:4356) |
| 239879 Red Hat Update for kernel-rt (RHSA-2021:4140) |
| 375284 EulerOS Security Update for kernel (EulerOS-SA-2021-1311) |
| 390233 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0005) |
| 610351 Google Pixel Android July 2021 Security Patch Missing |
| 670185 EulerOS Security Update for kernel (EulerOS-SA-2021-1684) |
| 670269 EulerOS Security Update for kernel (EulerOS-SA-2021-1808) |
| 750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1) |
| 750428 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0075-1) |
| 750434 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0060-1) |
| 900040 CBL-Mariner Linux Security Update for kernel 5.4.91 |
| 903286 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3722) |

906036 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3722-1)

940265 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](#)