



CVE-2019-20636

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-20636 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-04-08 14:15:00 UTC |
| Updated | 2023-11-09 13:57:00 UTC |
| Description | In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrate |

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|--|---------|--------|---------|----------|
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H300s | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H410s | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H500s | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H610c | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H610s | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H615c | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H700s | - | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Hardware | Netapp | Fas 8300 | - | All | All | All |
| Hardware | Netapp | Fas 8700 | - | All | All | All |
| Hardware | Netapp | Fas A400 | - | All | All | All |
| Hardware | Netapp | Fas Baseboard Management Controller A220 | - | All | All | All |
| Hardware | Netapp | Fas Baseboard Management Controller A320 | - | All | All | All |
| Hardware | Netapp | Fas Baseboard Management Controller A800 | - | All | All | All |
| Hardware | Netapp | Fas Baseboard Management Controller C190 | - | All | All | All |

| | | | | | | |
|-------------|------------------------|---|---|-----|-----|-----|
| Hardware | Netapp | H300s | - | All | All | All |
| Hardware | Netapp | H410s | - | All | All | All |
| Hardware | Netapp | H500s | - | All | All | All |
| Hardware | Netapp | H610c | - | All | All | All |
| Hardware | Netapp | H610s | - | All | All | All |
| Hardware | Netapp | H615c | - | All | All | All |
| Hardware | Netapp | H700s | - | All | All | All |
| Application | Netapp | Solidfire | - | All | All | All |
| Application | Netapp | Steelstore Cloud Integrated Storage | - | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|-------------------------------------|-----------------------|
| Input: add safety guards to input_set_keycode() · torvalds/linux@cb222ae · GitHub | MISC | github.com | Patch, Third Party |
| cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.4.12 | MISC | cdn.kernel.org | Release Notes, Vendor |
| April 2020 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org | Patch, Vendor Adv |
| [SECURITY] [DLA 2241-2] linux security update | MLIST | lists.debian.org | |
| [SECURITY] [DLA 2241-1] linux security update | MLIST | lists.debian.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)

[377053](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0028)

[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](#)