



# CVE-2022-0500

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

## Summary

<b>CVE</b>	CVE-2022-0500
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-25 19:15:00 UTC
<b>Updated</b>	2023-06-26 18:01:00 UTC
<b>Description</b>	A flaw was found in unrestricted eBPF usage by the BPF_BTFF_LOAD, leading to a possible out-of-bounds memory write in

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedora</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedora</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.17	-	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All

Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All

## References

### Reference

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[CVE-2022-0500 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[kernel/git/torvalds/linux.git - Linux kernel source tree](#)

[2044578 – \(CVE-2022-0500\) CVE-2022-0500 kernel: Linux eBPF logic vulnerability leads to critical memory read and write gaining root privileg](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[184526](#) Debian Security Update for linux (CVE-2022-0500)

[198861](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5518-1)

[198897](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5564-1)

[242890](#) Red Hat Update for kernel (RHSA-2024:0724)

[282441](#) Fedora Security Update for kernel (FEDORA-2022-952bb7b856)

[282445](#) Fedora Security Update for kernel (FEDORA-2022-edbd74424e)

[353964](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-001

[354327](#) Amazon Linux Security Advisory for kernel : ALAS2022-2022-083

[354468](#) Amazon Linux Security Advisory for kernel : ALAS2022-2022-185

[354542](#) Amazon Linux Security Advisory for kernel : ALAS-2022-185

[355199](#) Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

[355565](#) Amazon Linux Security Advisory for kernel : ALAS2KERNFI-5.15-2023-023

300000 Amazon Linux Security Advisory for kernel (ALAS-2022-1529)

377117 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)

610451 Google Pixel Android December 2022 Security Patch Missing

900796 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9271)

900902 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9241)

901332 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9271-1)

902055 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9241-1)

906223 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9271-2)

906393 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9241-2)

© [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](#)**