



# CVE-2021-31440

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

## Summary

<b>CVE</b>	CVE-2021-31440
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-21 15:15:00 UTC
<b>Updated</b>	2023-08-11 19:53:00 UTC
<b>Description</b>	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker n

## Risk And Classification

**Problem Types:** CWE-682

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	5.11.15	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	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="#">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

Hardware	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller</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	Tags
ZDI-21-503   Zero Day Initiative	MISC	<a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a>	
CVE-2021-31440 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="http://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canon

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159492</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
<a href="#">180577</a> Debian Security Update for linux (CVE-2021-31440)
<a href="#">198416</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)
<a href="#">198417</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)
<a href="#">198419</a> Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5001-1)
<a href="#">198426</a> Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)
<a href="#">239816</a> Red Hat Update for kernel security (RHSA-2021:4356)
<a href="#">239879</a> Red Hat Update for kernel-rt (RHSA-2021:4140)
<a href="#">353158</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002
<a href="#">610418</a> Google Pixel Android June 2022 Security Patch Missing
<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](https://status.cve.report)