



# CVE-2020-14305

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

## Summary

<b>CVE</b>	CVE-2020-14305
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-02 01:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	An out-of-bounds memory write flaw was found in how the Linux kernel's Voice Over IP H.323 connection tracking function:

## 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="#">Linux</a>	<a href="#">Linux Kernel</a>	4.12	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	4.12	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A250 Firmware</a>	-	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
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Fas 500f</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Fas 500f 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
[v4.10] netfilter: nf_contrack_h323: lost .data_len definition for Q.931/ipv6 - Patchwork	MISC	<a href="#">patchwork</a>
[OVZ-7188] Crash kernel 3.10.0-1062.4.2.vz7.116.7 - bugs.openvz.org	MISC	<a href="#">bugs.openvz.org</a>

[v4.10] netfilter: nf_contrack_h323: lost .data_len definition for Q.931/ipv6 - Patchwork		<a href="#">patchwork</a>
1850716 – (CVE-2020-14305) CVE-2020-14305 kernel: memory corruption in Voice over IP nf_contrack_h323 module	MISC	<a href="#">bugzilla</a>
CVE-2020-14305 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [375284](#) EulerOS Security Update for kernel (EulerOS-SA-2021-1311)
- [390217](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)
- [390234](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0001)
- [610344](#) Google Android Devices June 2021 Security Patch Missing
- [610354](#) Google Android July 2021 Security Patch Missing for LGE
- [610355](#) Google Android July 2021 Security Patch Missing for Samsung
- [610358](#) Google Android July 2021 Security Patch Missing for Huawei EMUI
- [670185](#) EulerOS Security Update for kernel (EulerOS-SA-2021-1684)
- [751451](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)

© [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](#)