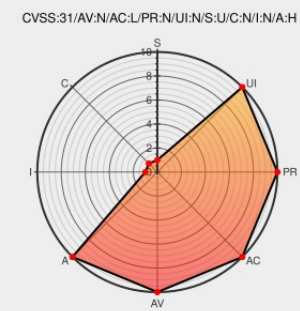
CVE-2021-38207

Published on: 08/08/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 12:23:00 PM UTC

CVE-2021-38207

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for about ten minutes.

CVE-2021-38207 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.13
CVE-2021-38207 Linux Kernel Vulnerability in NetApp Products |	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20210902-0007/

NetApp Product Security

net: ll_temac: Fix TX BD buffer overwrite · torvalds/linux@c364df2 · GitHub	github.com text/html	MISC github.com/torvalds/linux/commit/c364df2489b8ef2f5e3159b1dff1ff1fdb16040d

Related QID Numbers

198491 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5070-1)

198548 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5120-1)

671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688)

751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1)

751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)

751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)

900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1

900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-38207 : drivers/net/ethernet/xilinx/ll_temac_main.c in the #Linux #kernel before 5.12.13 allows remote att… twitter.com/i/web/status/1…	2021-08-08 20:05:14

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report