



CVE-2021-35039

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

Summary

CVE	CVE-2021-35039
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-07 01:15:00 UTC
Updated	2023-05-16 10:59:00 UTC
Description	kernel/module.c in the Linux kernel before 5.12.14 mishandles Signature Verification, aka CID-0c18f29aae7c. Without CON

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	T
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.14	CONFIRM	cdn.kernel.org	
CVE-2021-35039 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
oss-security - CVE-2021-35039: Linux kernel loading unsigned kernel modules via init_module syscall	MISC	www.openwall.com	
module: limit enabling module.sig_enforce · torvalds/linux@0c18f29 · GitHub	CONFIRM	github.com	
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	lists.debian.org	
oss-security - CVE-2021-35039: Linux kernel loading unsigned kernel modules via init_module syscall	MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178844	Debian Security Update for linux-4.19 (DLA 2785-1)
180262	Debian Security Update for linux (CVE-2021-35039)
670744	EulerOS Security Update for kernel (EulerOS-SA-2021-2502)
750887	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1076-1)
750953	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2645-1)
750963	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2687-1)
900096	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
901916	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6570-1)
903034	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4432)
905892	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4432-1)

© [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](#)