



x86/iopl: Cure TIF_IO_BITMAP inconsistencies

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2025-38100
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-03 09:15:23 UTC
Updated	2026-05-12 13:16:42 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: x86/iopl: Cure TIF_IO_BITMAP inconsistencies io_bitmap

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-476

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 d64b7b05a827
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 2dace5e016c9
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 aa5ce1485562
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 2cfcbe1554c1
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 b3b3b6366dc8
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 73cfcc844558f
CNA	Linux	Linux	affected ea5f1cd7ab494f65f50f338299eabb40ad6a1767 8b68e978718f
CNA	Linux	Linux	affected 5.5
CNA	Linux	Linux	unaffected 5.5 semver
CNA	Linux	Linux	unaffected 5.10.239 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.186 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.142 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.94 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.34 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.3 6.15.* semver
CNA	Linux	Linux	unaffected 6.16 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link
git.kernel.org/stable/c/aa5ce1485562f20235b4c759eee5ab0c41d2c220	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d64b7b05a827f98d068f412969eef65489b0cf03	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/2cfcbe1554c119402e7382de974c26b0549899fe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/b3b3b6366dc8eb5b22edba9adc4bfff3cdacfd64c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/2dace5e016c991424a3dc6e83b1ae5dca8992d08	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/8b68e978718f14fdcb080c2a7791c52a0d09bc6d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/73cfcc8445585b8af7e18be3c9246b851fdf336c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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