



drm/exynos: hdmi: report safe 640x480 mode as a fallback when no EDID found

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

Summary

CVE	CVE-2024-40916
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:14 UTC
Updated	2026-05-12 12:16:59 UTC

Description In the Linux kernel, the following vulnerability has been resolved: drm/exynos: hdmi: report safe 640x480 mode as a fallback

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: NVD-CWE-noinfo

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 348aa3d47e8bc2fa4e5b8079554724343631
CNA	Linux	Linux	affected a8cb3b072403ce0748d368278bc7ab87d15e
CNA	Linux	Linux	affected 912c149a52c37a2f8199449360bf392ae4ef7
CNA	Linux	Linux	affected 8f914db6fe252c5e78a9b8b03adc1b0a33aec
CNA	Linux	Linux	affected b71ae5fb2dd3c89c66efa613dccffc45c246c8
CNA	Linux	Linux	affected 13d5b040363c7ec0ac29c2de9cf661a24a8a:
CNA	Linux	Linux	affected 13d5b040363c7ec0ac29c2de9cf661a24a8a:
CNA	Linux	Linux	affected d930ab0399c350f9da9c64030daca368c78e:
CNA	Linux	Linux	affected 1cef1ef376c6421bb18e2185b5e10973bc272
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.95 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.35 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.6 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/799d4b392417ed6889030a5b2335ccb6dcf030ab	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/e23f2eaf51ecb6ab4ceb770e747d50c1db2eb222	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/6d6bb258d886e124e5a5328e947b36fdbcb3a6028	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co

git.kernel.org/stable/c/c3ca24dfe9a2b3f4e8899af108829b0f4b4b15ec	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/4dffb50316c761c59386c9b002a10ac6d7bb6c9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/35bcf16b4a28c10923ff391d14f6ed0ae471ee5f	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/510a6c0dfa6ec61d07a4b64698d8dc60045bd632	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.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