

CVE-2026-98566

Microsoft drm/imagination: clamp freelist reconstruction requests

In the Linux kernel, the following vulnerability has been resolved: drm/imagination: clamp freelist reconstruction requests The firmware reconstruction count controls accesses to the request's fixed freelist ID array and the copy into the fixed response array. Neither access currently bounds the count to those protocol arrays. Clamp the count to the request capacity, which is shared by the response layout, and use that count consistently for reconstruction and response publication.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.3rd percentile · FIRST	CISA DEADLINE — No CISA deadline
---	---------------------------------------	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 2 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☐ EPSS	0.002 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☐ CVSS	CVSS base score unavailable	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Monitor Untagged reference available; patch status is not confirmed

NVD lists one or more references for this CVE that aren't tagged as a patch or vendor advisory. Review them directly to confirm patch availability and applicability before making a remediation decision.

Basis: NVD reference (untagged)

Keep the firmware recovery exchange instead of dropping an oversized request without a response, as discussed with the firmware maintainer. The issue was found by our static-analysis tool.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Reference	git.kernel.org/stable/c/45585c3aa285854face65293acc95eff73063d6d	Additional reference	git.kernel.org/stable/c/b78f8f5532a077baa4aabccf657a4fb3b164659e
Additional reference	git.kernel.org/stable/c/e0560db0ea6e10c283ebe7c259a7af8d3b6e61a6	Additional reference	git.kernel.org/stable/c/eabd0ae3611769c826dbc118a1e240628731b348
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98566	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103611
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98566		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.