

CVE-2026-98658

Microsoft iio: proximity: aw96103: validate firmware data length

In the Linux kernel, the following vulnerability has been resolved: iio: proximity: aw96103: validate firmware data length The firmware parser reads a length from the binary header and then uses it to walk six-byte register/value entries. A truncated firmware image can make the parser read beyond the copied firmware buffer. A value smaller than the four-byte count field also underflows, producing a very large length. Read the little-endian field with `get_unaligned_le32()`, as previously proposed by David Lechner.

EVRS 0 /100 Informational priority	CVSS — Not scored	EPSS 0.002 9.2nd 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)

Validate the header size, reject an underflowed length, ensure the resulting payload is contained in the firmware image, and require it to contain whole register/value entries.

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/1a7c522a35477d70320bd64aba8e9de0c1058c6f	Additional reference	git.kernel.org/stable/c/4a9b9f2d4e26589afd0ac099c8e5593170dd5ac7
Additional reference	git.kernel.org/stable/c/6501b032be217ecf47e793b78a05078cf0b604ad	Additional reference	git.kernel.org/stable/c/815ae0b73b69ace207b6bbf7ef428b06491c3ddb
NVD	nvd.nist.gov/vuln/detail/CVE-2026-98658	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-103912
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-98658		

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