Missing Authentication for Critical Function vulnerability in Anritsu Remote Spectrum Monitor

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3356
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 19:16:28 UTC
Updated	2026-04-01 14:23:37 UTC
Description	The MS27102A Remote Spectrum Monitor is vulnerable to an authentication bypass that allows unauthorized users to acce

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000540000 probability, percentile 0.172560000 (date 2026-04-02)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing authentication for critical function

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Anritsu	Remote Spectrum Monitor MS27100A	affected All versions custom	Not specified
CNA	Anritsu	Remote Spectrum Monitor MS27101A	affected All versions custom	Not specified
CNA	Anritsu	Remote Spectrum Monitor MS27102A	affected All versions custom	Not specified
CNA	Anritsu	Remote Spectrum Monitor MS27103A	affected All versions custom	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/news-events/ics-advisories/icsa-26-090-01	ics-cert@hq.dhs.gov	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Souvik Kandar (en)

Additional Advisory Data

Workarounds

CNA: Anritsu has no plans to fix this issue. Anritsu recommends that users deploy Remote Spectrum Monitor within secure network environments to mitigate potential risks. Users can contact Anritsu Technical Support (1-800-267-4878) for more information.

There are currently no legacy OID mappings associated with this CVE

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

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