

CVE-2021-27561

Yealink Device Management Server-Side Request Forgery (SSRF) Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Yealink Device Management (DM) 3.6.0.20 allows command injection as root via the /sm/api/v1/firewall/zone/services URI, without authentication.

EVRS 82 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.829 99.67th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.829 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
device management	≤ 3.6.0.20	after 3.6.0.20	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-743m-83p4-9349	NVD	nvd.nist.gov/vuln/detail/CVE-2021-27561
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-14312
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-27561		

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