

CVE-2023-25717

Ruckus Wireless Multiple Ruckus Wireless Products CSRF and RCE Vulnerability

Exigent

CISA KEV since May 12, 2023

Actively exploited

Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a `/forms/doLogin?login_username=admin&password=password$(curl substring)`.

EVRS 87 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.981 99.91st percentile · FIRST	CISA DEADLINE Jun 2, 2023 KEV since 2023 · 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	0.981 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions or disconnect product if it is end-of-life.

Basis: CISA KEV required action

Affected and fixed versions · 53 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ruckus wireless admin	≤ 10.4	after 10.4	NVD
smartzone ap	< 6.1.0.0.9240 < 5.2.2.0.2064 < 3.6.2.0.795 < 6.1.1.0.1274	6.1.0.0.9240 · 5.2.2.0.2064 · 3.6.2.0.795 · 6.1.1.0.1274	NVD
ruckus smartzone firmware	< 5.2.1.3 6.1.0.0.935 < 5.2.1.3.1695	5.2.1.3	NVD
e510	—	no fixed version listed	NVD
h320	—	no fixed version listed	NVD
h350	—	no fixed version listed	NVD
h510	—	no fixed version listed	NVD
h550	—	no fixed version listed	NVD

Sources

Vendor guidance	support.ruckuswireless.com/security_bulletins/315	NVD	nvd.nist.gov/vuln/detail/CVE-2023-25717
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-29627
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-25717		

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