

CVE-2022-20821

Cisco IOS XR Open Port Vulnerability

CISA KEV since May 23, 2022

Actively exploited

A vulnerability in the health check RPM of Cisco IOS XR Software could allow an unauthenticated, remote attacker to access the Redis instance that is running within the NOSi container. This vulnerability exists because the health check RPM opens TCP port 6379 by default upon activation. An attacker could exploit this vulnerability by connecting to the Redis instance on the open port.

EVRS 75_{/100} Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.115 96th percentile · FIRST	CISA DEADLINE Jun 13, 2022 KEV since 2022 · 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	0.115 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ 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

A successful exploit could allow the attacker to write to the Redis in-memory database, write arbitrary files to the container filesystem, and retrieve information about the Redis database. Given the configuration of the sandboxed container that the Redis instance runs in, a remote attacker would be unable to execute remote code or abuse the integrity of the Cisco IOS XR Software host system.

Affected and fixed versions · 20 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios xr	—	no fixed version listed	NVD
8201	—	no fixed version listed	NVD
8202	—	no fixed version listed	NVD
8208	—	no fixed version listed	NVD
8212	—	no fixed version listed	NVD
8218	—	no fixed version listed	NVD
ncs-55a1-24h	—	no fixed version listed	NVD
ncs-55a1-24q6h-s	—	no fixed version listed	NVD

Sources

Vendor guidance	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-redis-ABJyE5xK	NVD	nvd.nist.gov/vuln/detail/CVE-2022-20821
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-26071
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-20821		

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