

CVE-2020-3566

Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A vulnerability in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to exhaust process memory of an affected device. The vulnerability is due to insufficient queue management for Internet Group Management Protocol (IGMP) packets. An attacker could exploit this vulnerability by sending crafted IGMP traffic to an affected device.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.6 High · NVD	EPSS 0.037 89.7th percentile · FIRST	CISA DEADLINE May 3, 2022 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	0.037 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ 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 cause memory exhaustion, resulting in instability of other processes. These processes may include, but are not limited to, interior and exterior routing protocols. Cisco will release software updates that address this vulnerability.

Affected and fixed versions · 2 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios xr	6.4.2	no fixed version listed	NVD
asr 9001	—	no fixed version listed	NVD
asr 9006	—	no fixed version listed	NVD
asr 9010	—	no fixed version listed	NVD
asr 9901	—	no fixed version listed	NVD
asr 9904	—	no fixed version listed	NVD
asr 9906	—	no fixed version listed	NVD
asr 9910	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-mr9v-hqhx-vq2j

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

NVD nvd.nist.gov/vuln/detail/CVE-2020-3566

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-24837

Current data evulnable.com/vulnerability-management/cve/CVE-2020-3566

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