# CVE Detail – CVE-2020-3566

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. 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.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.95028

## CVSS Scoring

CVSS v3.1 Score: 8.6

Severity: HIGH

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-400: Uncontrolled Resource Consumption
* CWE-770: Allocation of Resources Without Limits or Throttling

## CAPEC(s)

* CAPEC-125: Flooding
* CAPEC-130: Excessive Allocation
* CAPEC-147: XML Ping of the Death
* CAPEC-197: Exponential Data Expansion
* CAPEC-227: Sustained Client Engagement
* CAPEC-229: Serialized Data Parameter Blowup
* CAPEC-230: Serialized Data with Nested Payloads
* CAPEC-231: Oversized Serialized Data Payloads
* CAPEC-469: HTTP DoS
* CAPEC-482: TCP Flood
* CAPEC-486: UDP Flood
* CAPEC-487: ICMP Flood
* CAPEC-488: HTTP Flood
* CAPEC-489: SSL Flood
* CAPEC-490: Amplification
* CAPEC-491: Quadratic Data Expansion
* CAPEC-492: Regular Expression Exponential Blowup
* CAPEC-493: SOAP Array Blowup
* CAPEC-494: TCP Fragmentation
* CAPEC-495: UDP Fragmentation
* CAPEC-496: ICMP Fragmentation
* CAPEC-528: XML Flood

## ATT&CK Techniques

* T1498.001: Direct Network Flood
* T1499.001: OS Exhaustion Flood
* T1499.003: Application Exhaustion Flood
* T1498.002: Reflection Amplification
* T1499.002: Service Exhaustion Flood
* T1499: Endpoint Denial of Service

## Used By (Actors/Tools)

* OnionDuke (malware)
* ZxShell (malware)
* Sandworm Team (intrusion-set)

## Affected Products

* cpe:2.3:o:cisco:ios\_xr:6.4.2:\*:\*:\*:\*:\*:\*:\*