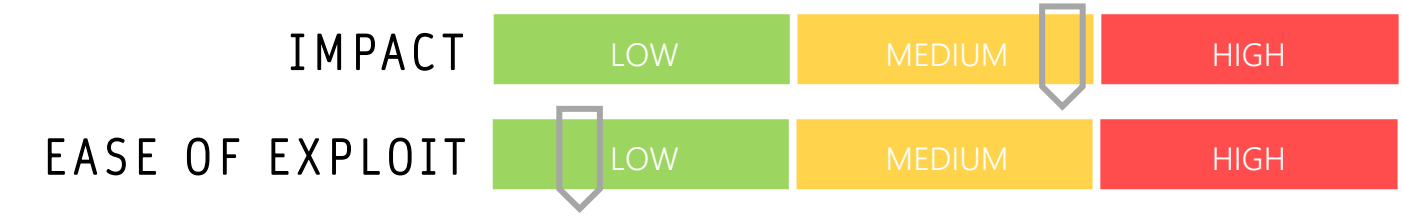
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00030

ACTIVE EXPLOITATION OF CISCO ROUTERS

DATE ISSUED: 3rd September 2020



OVERVIEW

A number of vulnerabilities in Cisco IOS XR Software through the Distance Vector Multicast Routing Protocol (DVMRP) feature has the potential to allow unauthorised remote access to its carrier-grade routers. As a result, attackers have the power to crash devices through the over-consumption of memory and exploiting the Internet Group Management Protocol (ICMP) and crashing other processes.

BREAKDOWN

This flaw is known to be present in any Cisco device running any release of IOS XR with multicast routing configured to an active interface, or receiving traffic using DVMRP. The problem occurs in the handling and queuing of IGMP packets, which normally assist with maintaining network traffic efficiency. If an attacker is able to send IGMP packets to a vulnerable device, they may be successful in exhausting available memory resources, leading to processes becoming unstable and crashing, affecting both internal and external routing capabilities. For more information please see CVE-2020-3566,

REMEDIATION STEPS

- Cisco is currently working on a remediation and in the meantime recommends the following mitigations:
  - Apply a rate limiter to assist with understanding a baseline of IGMP traffic and to set corresponding limits deemed acceptable on the network.
  - Restart the IGMP process to regain memory consumed
  - Implement Access Control Entry (ACE) to Access Control Lists (ACLs) on an existing interface or create a new ACL to deny DVMRP traffic over that interface

REFERENCES & RESOURCES

Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

Threatpost: https://threatpost.com/cisco-warns-of-active-exploitation-of-flaw-in-carrier-grade-routers/158887/