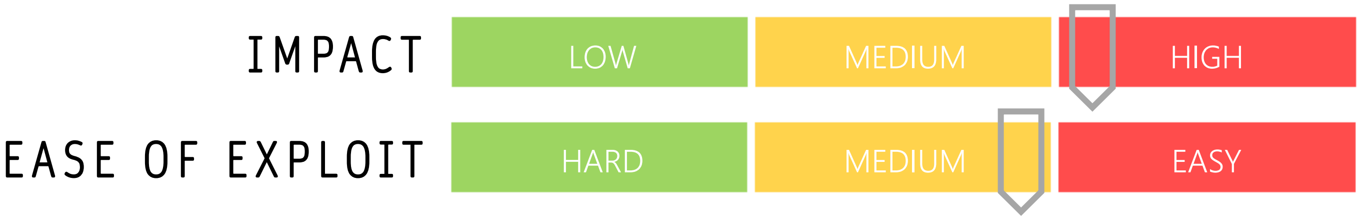
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00069

DOS FLAW IN CISCO ASR ROUTERS

DATE ISSUED: 16th November 2020



OVERVIEW

Cisco’s Aggregation Service Routers (ASR) have a known vulnerability in the ingress packet processing function whereby an attacker can gain remote, unauthenticated access and potentially bring down the system in a Denial of Service (DoS) buffer overflow attack,

BREAKDOWN

The flaw based in the widely used Cisco Internetwork Operating System (IOS) XR software may make the ASR9000 series routers vulnerable to a buffer overflow style attack. By overloading the system’s buffer resources, routers would be unable to process or forward any incoming traffic resulting in a DoS. Using Layer 2 and Layer 3 protocol in a heavy stream, the attacker would be able to exhaust the buffer resources, resulting in system crash. The error message ”%PKT_INFRA-spp-4-PKT_ALLOC_FAIL : Failed to allocate n packets for sending” could be an indication the device is under attack.

REMEDIATION STEPS

- Contact your Cisco Customer Support agent if this issue is encountered
- Restart any device suffering for packet forwarding errors
- Ensure that Cisco ASR 9000 routing devices are running the latest IOS version (6.7.2+ and 7.1.2+)
- Employ load balancing and filtering the ease the load for router packet processing
- Conduct network monitoring to alert any suspicious behaviours such as high volumes of traffic or traffic types from a single location

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/high-severity-cisco-dos-flaw-asr-routers/161115/
Cisco	https://www.cisco.com/c/en/us/support/routers/asr-9000-series-aggregation-services-routers/products-security-advisories-list.html