https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10343#

Keywords or Article ID... × Search

Denial of Service Vulnerability for certain MPLS Packets (VU#409555, CVE# CAN-2004-0467)

[JSA10343] Show Article Properties

LEGACY ADVISORY ID:

PSN-2005-02-004

PRODUCT AFFECTED:

All M-series and T-series routing platforms

PROBLEM:

(NOTE: This document updates and supersedes PSN-2005-01-010)

When an M-series or T-series Juniper routing platform receives certain MPLS packets, the packets are immediately delivered to the Routing Engine (RE) for further processing. This occurs even if packets are received on an interface which is not enabled for MPLS processing, or if the router is not configured to process MPLS packets at all. Furthermore, these MPLS packets are delivered without any further processing by the hardware, thus bypassing all attempts at limiting the number of, or otherwise filtering, the packets. A large stream of these MPLS packets can overload internal communication paths and interfere with the timely processing of other packets.

As a result, packets associated with routing protocols, link-layer management, and network traffic terminating on the router can be interrupted. Routing protocol adjacencies may be lost, telnet and ssh sessions may stall or time out, or interfaces may appear to "flap" for no apparent reason. The packet stream therefore creates a Denial of Service attack against the routing platform.

Symptoms of an attack in progress might include CPU utilization on the RE being somewhat higher than usual, however the utilization will not typically reach levels high enough to trigger alarms. Traffic rates on the internal fxp1 interface that connects the RE to the Packet Forwarding Engine (PFE) will approach its maximum capacity.

This vulnerability can be exploited by an attacker directly attached to a Juniper Networks M-series or T-series routing platform, even if the interface to which the attacker is attached is not enabled for MPLS. An attacker not directly attached to the routing platform can exploit this vulnerability on transit Label Switch Routers within an Internet Service Provider's MPLS-enabled core network.

This vulnerability is specific to Juniper Networks M-series and T- series routers running JUNOS software releases built prior to January 6, 2005. J-series routers and routers that do not run JUNOS software are not susceptible to this vulnerability. Juniper Networks is not aware of any actual or attempted exploit of this vulnerability.

Juniper Networks would like to thank Qwest Communications and their Software Certification team for identifying this issue as a security vulnerability within Juniper Networks products.

SOLUTION:

The JUNOS software has been modified to limit the volume of MPLS traffic forwarded to the Routing Engine, thereby preventing these packets from consuming all bandwidth on the internal communication path. Additional software changes were made to completely ignore MPLS packets arriving on non-MPLS-enabled interfaces.

All versions of JUNOS software built on or after January 20, 2005 contain the modified code. Software built between January 6 and January 20 may contain the modified code, depending on the specific JUNOS release.

IMPLEMENTATION:

All customers are strongly encouraged to upgrade their software to a release that contains the modified code. Pointers to software releases with the corrected code can be found in the Related Links section below. Customers can also contact Juniper Network's Technical Assistance Center for download assistance.

As a partial work-around, either of the no-decrement-ttl or the no-propagate-ttl configuration options can be used to reduce the exposure to this vulnerability from remote attackers. These configuration options prevent the attacker from affecting transit Label Switch Routers (LSR) in the Service Provider's core network. However, the configuration options do not protect against directly- attached attackers, nor do they protect the egress LSRs in an RFC2547bis Layer-3 Virtual Private Network environment.

Important Note! Use of these configuration knobs on M-series routers can introduce anomalous MPLS TTL behavior when the router is running JUNOS release 6.4 or 7.0. IPv4 packets that transit an MPLS core network can leave an LSP with a TTL value greater than when the packet entered the LSP. This anomolous TTL behavior is a regression created by an unrelated change in the code, and is tracked within Juniper as PR/56025.

RELATED LINKS:

- Software Download Links
- CERT/CC Vulnerability Note VU#409555

RISK LEVEL:

High

RISK ASSESSMENT:

Both directly-attached and remote attackers can severely disrupt normal operation of the routing platform. Exposure to remote attackers can be reduced (but not eliminated) by certain router configuration options; however, attacks from directly-attached devices cannot be averted by simple configuration options.