



Intrusion Prevention System Release Notes

Version 3.9.5

To ensure that you have the latest versions of product documentation, visit the [Online Help Center](#).

Important notes for IPS

- Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required. This ensures a successful upgrade and allows for a TOS rollback, if necessary. You can remove previous TOS versions using the SMS, the LSM, or the CLI.
- After installing this release, update the DV package to the latest version.
- Use SMS v5.0.1 Patch 2 or later to manage a device with this release.

Release Contents

Description	Reference
This release addresses the following vulnerabilities affecting the NX-Series management network port: CVE-2019-12255, CVE-2019-12258, and CVE-2019-12263. For more information about this issue refer to Product Bulletin #1080 .	40306

Known issues

Description	Reference
Reference Devices configured to connect to an NTP server using the server hostname no longer connect to the NTP server after a reboot. To avoid this issue, always establish an NTP server connection using the IPv4/ IPv6 address of the NTP server.	118020
Microsoft Edge or Microsoft Internet Explorer might not connect to the LSM. To resolve this issue, use the <code>conf t server TLS</code> command to enable TLS v1.0 on the IPS security device. Be aware that TLS v1.0 is a weak encryption algorithm. Consider using another supported browser instead. For more information about using the <code>conf t server</code> command, refer to the <i>IPS Command Line Interface Reference</i> .	117878
A profile distribution issue can degrade system performance, including dropped packets and a spike in XLR utilization. A filter reset temporarily clears the condition.	124604
Modifying a profile or changing which profile is applied to the ANY-ANY virtual segment of a device, <i>while that device is unmanaged from SMS</i> , can cause an out-of-sync condition when the device is remanaged to the SMS. The recovery for the out-of-sync condition is to reboot the device. To avoid this condition, make changes to the ANY-ANY virtual segment only through the SMS.	124603
Common CIDRs, such as /56 and /64, cannot be used for IPv6 bypass rules.	124529

Product support

For assistance, contact the [Technical Assistance Center \(TAC\)](#).

© Copyright 2019 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks of their respective owners.