



# IPS Engine - Release Notes

Version 5.2

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Product integration and support</b> .....	<b>6</b>
<b>Resolved issues</b> .....	<b>7</b>
Common Vulnerabilities and Exposures .....	8
<b>Known issues</b> .....	<b>9</b>

# Change log

Date	Change Description
2022-08-08	Initial release.
2023-12-04	Updated <a href="#">Resolved issues on page 7</a> .

# Introduction

This document provides the following information for the Fortinet IPS Engine 5.2 build 267.

- [Product integration and support on page 6](#)
- [Resolved issues on page 7](#)
- [Known issues on page 9](#)

IPS Engine 5.2 build 267 is a built-in release for FortiOS 6.2.11. It is not a release to FortiGuard.

For additional FortiOS documentation, see the [Fortinet Document Library](#).

# Product integration and support

The following table lists IPS engine product integration and support information:

<b>FortiOS</b>	6.2.11
----------------	--------

# Resolved issues

The resolved issues listed do not list every bug that this release corrects. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
698247	Flow mode Web Filter override crashes and socket leaks in IPS daemon.
713508	Low download performance when SSL deep inspection is enabled on aggregation + VLAN interface when nTurbo is enabled.
752466	Deep inspection causes downloads to fail in ADVPN environment.
752559	IPS engine crashes with signal 11.
754579	Application performance is ten times worse when IPS Engine is applied in flow mode.
755223	There is no detection trigger packet in PCAP.
755294	Firefox displays <code>SEC_ERROR_REUSED_ISSUER_AND_SERIAL</code> error when ECDSA CA is configured for deep inspection.
756398	An invalid character string is inserted in the IPS engine log sent to the TCP SYSLOG server.
757314	IPS Engine crashes after upgrade, affecting traffic.
759194	FortiGate inserts wrong timestamp into PCAP data.
760555	Web Filter UTM logs unexpected URL such as <code>url="https://"</code> .
765859	Repeated IPS engine signal 11 and signal 7 crashes.
774826	IPS engine processes consume high CPU usage.
775566	Websites do not load in flow mode with deep SSL inspection.
777464	Update crashes after running scripts.
780194	IPS engine signal 14 alarm clock crashes during stress testing.
786479	Traffic log does not work under next generation firewall mode while a reboot can solve the issue on FortiGate 101E.
787151	FortiGate inserts epoch time into the PCAP when detected by some signatures.
792312	HTTPS traffic cannot pass FortiGate-VM on VMware ESXi well when IPS engine and deep inspection are enabled.
801575	IEC.61850 and MMS signatures do not work.
802465	<code>ERR_SSL_PROTOCOL_ERROR</code> occurs when loading a website in flow mode.

## Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	Description
797229	IPS Engine 5.2 build 267 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2022-27491</li></ul>

## Known issues

There are no known issues with this release of IPS engine 5.2 build 267 for FortiOS 6.2.4 and later versions.

To report a bug, please contact [Customer Service & Support](#).



**FORTINET**<sup>®</sup>



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.