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

December 04, 2023
IPS Engine 5.2 Release Notes
43-520-778319-20231204

TABLE OF CONTENTS

Change log

Date	Change Description
2022-08-08	Initial release.
2023-12-04	Updated Resolved issues on page 7.

Introduction

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

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:

FortiOS	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 `SEC_ERROR_REUSED_ISSUER_AND_SERIAL` 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 `url="https:///"`.
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	ERR_SSL_PROTOCOL_ERROR 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: • CVE-2022-27491

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.