AV Engine for FortiOS - Release Notes

Version 6.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 01, 2019
AV Engine for FortiOS 6.0 Release Notes
44-600-536735-20190201

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-02-01	Initial release.

Introduction

This document provides the following information for the Fortinet AV Engine 6.0 build 0019.

- What's new in AV Engine 6.0 build 0019 on page 6
- Product integration and support on page 7
- Resolved issues on page 8

For additional FortiOS documentation, see the Fortinet Document Library.

What's new in AV Engine 6.0 build 0019

New features

- The AV engine can now identify, decompress, and scan compiled HTML (.CHM) files.
- Changed AV scan logic to keep looking for malware if a file is found to contain grayware.
  Previously, if grayware scanning was enabled and the AV engine found grayware, it would stop scanning. Now, if grayware is found, the scanner continues looking for malware. This change should improve malware statistics gathering.
- The AV engine can now identify and scan IQY files, and can send these files to FortiSandbox.

Enhancements

- Improved the information available for users in files that have been cleaned and reconstructed by the Content Disarm and Reconstruction (CDR) feature.
- Upgraded support for identifying and scanning Microsoft compound file binary files.
- Upgraded support for identifying and scanning DotNet files.

Product integration and support

Fortinet product support

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

FortiOS	6.0.0 and later

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, contact Customer Service & Support.

AV engine fixes

Bug ID	Description
454103	Resolved an issue that caused DLP to block zip files when configured to block .bat files.
459010	The AV engine can now successfully decompress FlateDecode streams in NSS PDF samples.
475571	Resolved an issue that would sometimes cause the AV engine incorrectly identify .exe files as corrupted sfx zip files.
478135	Resolved an issue related to CPRL LOC buffers.
479444	Resolved an issue that prevented the AV engine from identifying some OLE files.
485202	Resolved an issue that prevented the AV engine from identifying some sfx zip files.
485788	Resolved an issue that caused the DEX parser to crash.
487535, 489308	Resolved issues with the Java Script emulator that caused the AV engine to crash or not identify infected samples.
489438	Resolved an issue that caused the AV engine to find incorrect file sizes during AV_VIRINFO_WMCKSUM processing.
492624	Resolved an issue with PRC file typing that caused DLP to block websites that should be allowed.
493884	Resolved an issue that would sometimes cause the AV engine to flag zip64 samples as corrupted.
494824	Resolved an issue that caused the AV engine to sometimes crash when scanning cfb files.
496255	Resolved an issue that caused some XML-based MS Office files to be identified as zip files.
496255	Resolved an issue that caused the AV engine to sometimes mistake XML-based MS Office files for ZIP files.
498679	Improved identification of corrupted zip files.
500918	Resolved an issue that caused the AV engine to crash when decompressing RTF files.
502933	Resolved a pattern matching issue that prevented some infections from being detected.
503014	Resolved an issue that caused the AV engine to timeout when scanning ARJ archives that contained large files (ARJ bombs).

Bug ID	Description
504187	Resolved an issue that caused DLP to incorrectly block PDF files that were found to contain MIME content.
510563	Increased the structured exception handling (SEH) limit to allow unpacking of files with an excessive number of SEH handlers.
511060	Resolved an issue that sometimes caused the AV engine to crash when scanning zip files.
514312	Resolved an issue with how the AV engine handles extracted file names that contain invalid characters.
514514	Resolved an issue that sometimes prevented CDR from adding a cover page to a recovered PDF file.
514654	Resolved an issue that caused the AV engine to timeout when uncompressing XZ files when the resulting uncompressed file would be larger than the file size limit.