WEB APPLICATION FIREWALL

FortiWeb™ 5.0 Patch 1

Release Notes

FortiWeb™ 5.0 Patch 1 Release Notes

July 26, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides installation instructions and caveats, resolved issues, and known issues for FortiWeb™ 5.0.1, build 0039.

FortiWeb provides web application security in a single platform enabling the protection, load balancing and acceleration of web applications and the data exchanged between them and clients.

For additional documentation, please visit:

http://docs.fortinet.com/fweb.html

What's new

Site publishing

Primarily focused on Microsoft applications though not only, the new Site Publishing feature provides the ability to easily publish Outlook Web Access (OWA), SharePoint and Lync applications. FortiWeb streamlines authentication to the different applications and provides SSO functionality

"Alert Only" status for single signature

It is now possible to move single signatures to "Alert Only" status. Allows for better tuning flexibility by not forcing administrators to disable a signature that causes multiple false positives

Attack signature filters

New filters have been added to the Advanced mode Signatures tab. Filter for signatures that have been disabled or moved into "Alert Only" status

Custom Global White List

Add your own URLs, parameters and cookies that you don't want FortiWeb to inspect. Complements the Predefined Global White List.

Advanced Protection Custom Rule enhancement

Regular expressions are now supported in Advanced Protection Custom Rule HTTP Header filter

New CLI debugging commands

New command to debug the SNMP daemon- 'diagnose debug application snmp' and command to view disk read-only error logs – 'diagnose debug emerglog'

Memory optimization

Performance enhancement to memory utilization

Antivirus enhanced

The Antivirus database now only loads to memory when antivirus is used in a policy,

GeoLite new format supported

The new GeoLite DB format is now supported

Access to OS shell

It is now possible to access the operating system's shell in release builds using the command 'sysctl sh'

Change & performance notices

Viewing logs after upgrading

Due to log format change in FortiWeb 5.0 events created in FortiWeb 4.x are not automatically presented. To view old events go to the Attack/Traffic tab, click on Log Management and choose the relevant log file. Pre 5.0 events cannot be presented in 5.0 reports.

Traffic logs & system health

Due to high volume of disk writing causing disk wear and tear and performance implications it is recommended to enable Traffic logs only while debugging problems. Disable traffic logs when in normal operations

Performance on FortiWeb 400B

Due to the 1GB memory limit on the FortiWeb 400B, customers using that model should use no more than 6 policies.

Performance & data analytics

Depending on how much data was gathered, data analytics queries can take some time. It is recommended to filter the data for short periods of time.

Data analytics data set limitations

Due to the large amount of data that can be stored in the data analytics database, for performance reasons, a data analytics query currently will only search up to 1,000,000 records at a time. This will be enhanced in the future.

Signature restructure

After upgrading to FortiWeb™ 5.0.1 from FortiWeb 4.x, review your existing web protection profiles. Pre-FortiWeb 4.0 MR4 signatures cannot be automatically converted to the new signature framework in FortiWeb 4.0 MR4. Due to this, during the upgrade, FortiWeb will automatically ***replace*** references to the old signatures with the predefined *Alert Only* attack and data leak signature sets.

You can either use this or another predefined signature set, or create and apply a new signature set. Notice this only applies when upgrading from pre FortiWeb 4.0 MR4 versions.

If you do not reconfigure each web protection profile's *Signatures* setting after the upgrade, many attacks and data leaks will ***not*** be blocked.

Upgrade instructions

Hardware & VM support

FortiWeb™ 5.0.1 supports:

- FortiWeb 400B
- FortiWeb 400C
- FortiWeb 1000B
- FortiWeb 1000C
- FortiWeb 3000C/3000CFsx
- FortiWeb 3000D/3000DFsx
- FortiWeb 4000C
- FortiWeb 4000D
- FortiWeb-VM

Upgrading from previous releases

Depending on which FortiWeb firmware version you are currently running, the recommended update path varies. Use the one that matches your firmware.

To upgrade from any release prior to FortiWeb 3.0 MR2

1. Upgrade to FortiWeb 3.0 MR2 Patch x.
   Note: Please review the release note when upgrading to FortiWeb 3.0 MR2 Patch x due to disk storage changes which impact the upgrade process.
2. Depending on your model, repartition (see Repartitioning the hard disk)
3. Upgrade to FortiWeb™ 5.0.1.

To upgrade from FortiWeb 3.0 MR3 Patch x

1. Depending on your model, repartition (see Repartitioning the hard disk)
2. Upgrade to FortiWeb™ 5.0.1

To upgrade from FortiWeb 3.0 MR3 special builds 8561 or 8562

1. Depending on your model, repartition (see Repartitioning the hard disk)
2. Upgrade FortiWeb™ 5.0.1

To upgrade from FortiWeb 4.0 MR4

1. Upgrade to FortiWeb™ 5.0.1 directly

If you do not update the firmware in this order, your configuration may not be correctly converted to be compatible with the new firmware. If you skip a repartition image, this can cause stability issues. Some features may not work, or will be unable to store data.

Repartitioning the hard disk

Before upgrading from FortiWeb 4.0 MR3 to FortiWeb 4.0 MR4 or greater, some models require that you adjust their partition sizes:

- FortiWeb-400B
- FortiWeb-1000B
- FortiWeb-1000C
- FortiWeb-3000C

Other models do not require repartitioning.
Note: Repartitioning affects the operating system's disk (USB/Flash disk), not the hard disk. Existing Event/Traffic/Attack logs, which are on the hard disk, will not be affected.

To repartition the hard drive

2. Back up FortiWeb's configuration and data. The partitioning procedure will automatically save your FortiWeb configuration. However, backups are a recommended best practice to prevent data loss in case of unexpected issues during the repartition.
3. Download the special partitioning image from the Fortinet Customer Service & Support site to your computer.
4. Install the partitioning image like you're installing/upgrading a normal firmware image using either the GUI (*System >Maintenance > Backup & Restore*) or CLI (`execute restore image`).
   If you use the CLI, these messages will appear:
   ```
   System is started.
   The flash is using 40M data image, need enlarge to 200M
   backup data disk 1 success
   mount /dev/sdb2 failed
   format disk /dev/sdb3 success
   restore backup files /tmpdisk1.tar->/dev/sdb1 success
   FortiWeb login:
   ```
5. Once the previous step is finished and the prompt is shown install FortiWeb™ 5.0 as usual.

Upgrading an HA cluster

If you have a FortiWeb model that requires the repartitioning procedure (see Repartitioning the hard disk) you must temporarily disable HA and upgrade each node individually, then re-enable HA.

If your model does ***not*** need re-partitioning:

- If the HA cluster is running FortiWeb 4.0 MR4, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it will automatically upgrade the standby appliance too. No manual intervention is required to upgrade the other appliance.
- If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, HA will not automatically propagate the firmware to the other appliance. However, you can still upgrade the HA cluster without temporarily disabling HA.

To upgrade a FortiWeb 4.0 MR3 Patch x HA cluster without disabling HA

1. Log in to the active appliance and upgrade it.
2. Wait for it to shut down and begin rebooting.
   In the CLI, you should see messages such as `The system is going down NOW !!`.
   In the GUI, if you quickly refresh your browser, you will be prompted again for your user name and password. This login, however, should be to the standby appliance, which you

can verify either by examining the host name in `get system status` in the CLI, or by the *System Information* widget *System* > *Status* > *Status* in the GUI.

3. Quickly log in to the standby unit and upgrade it.
4. While the standby appliance is upgrading, the original active appliance should return to its original role in the HA cluster.

Policies defined with priority deleted upon upgrade

In FortiWeb 5.0 the priority field has been removed. Priority is defined by the ID field. During the upgrade policies defined with priorities will be deleted. Delete the priority before upgrading in order to not have them deleted.

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, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
210998	Memory leak when auto learning was enabled.
0205587	Memory leak under heavy load.
0213291	No traffic/attack log after certain amount of time and under traffic load
0207138	Incorrect MAC address after enabling/disabling interface when in bound state.
0208761	Could not access FortiWeb using the default IP after factory reset.
205488	ntpd crashed intermittently.
209918	TCP RST sent incorrectly in transparent inspection mode.
210037	Memory leak when ‘stop monitor’ status was enabled.
0210320	Importing local certificate failed.
0210169	Fragmented packet caused cookie poisoning detection false positive.
0210698	FortiWeb did not forward the response when the HTTP response code was ‘100 Continue’.
210484	Performance issues in offline mode.
200326	Policy session maximum incorrect for FortiWeb 3000D/4000D.
211720	Memory leak when in certain conditions.
206020	System upgrade failed due to too many error logs.
0211739	GUI does not accept '+' (plus) sign in a signature exception's regular expression.
212403	Packets not monitored in transparent inspection mode when certain load is reached.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
168559	When deployed in offline detection mode, antivirus scanning does not function properly if the uploaded file is larger than 120 KB.
171436	HA member negotiation issues.
0205581	Unable to add an HTTP protocol constraint exception for malformed requests when the URL is too large.
206986	Incorrect site status for anti defacement.
212114	VM workstations' ARP entries disappear.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, go to *Download* > *Firmware Image Checksums*. In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool