Release Notes

FortiDDoS-F 6.3.5

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July 15, 2024
FortiDDoS-F 6.3.5 Release Notes
00-620-730305-20230228

TABLE OF CONTENTS

Change Log

Date	Change Description
July 15, 2024	FortiDDoS-F 6.3.5 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.3.5 build 0333.

FortiDDoS Release 6.3.5 has been issued to fix a known CVE. The underlying 6.3.x code is several releases out of date. Please upgrade to the latest GA Release.

Before upgrading, place FortiDDoS into Bypass mode using CLI:

```
Fortiddos #execute bypass-traffic enable
This operation will enable traffic bypass!
Do you want to continue? (y/n) y
```

There is a known issue during reboot where traffic is bypassed but the bypass is removed for 5-15 seconds before the processors are ready to process traffic as the system returns to normal.

It is recommended to perform upgrades in a maintenance window to avoid disrupting other network settings such as OSPF, RSTP and BGP that affect traffic when the physical ports are changed from inline to bypass and back to inline.

After upgrade is complete (GUI and all Dashboard panels are displaying):

```
Fortiddos #get system bypass status
```

`Normal` (system is inline and processing)

`Bypass` (system remains in bypass and requires manual return to inline below)

```
execute bypass-traffic disable
This operation will disable traffic bypass!
Do you want to continue? (y/n) y
```

Ensure to clear your browser cache (or operate in incognito mode) after a firmware upgrade. The GUI is coded in JSON in the browser and code changes in the system do not automatically signal the browser to rebuild the GUI. Changes to the GUI will not appear until the cache is cleared. If the cache is not cleared, you may see misaligned tables or entire Dashboard panels missing or appearing in the wrong place.

After upgrading from 6.1.x or 6.2.x to FortiDDoS-F 6.3.x, please check the integrity of the system Service Protection Policies (SPPs) and repair if necessary. See After upgrade on page 13 for checks to be completed post upgrade.

In early FortiDDoS-F-Series releases, the Round-Robin Databases (RRDs) were created automatically for each SPP whenever the user created a new SPP via the GUI or CLI. However, if the user makes a configuration change to the SPP while the RRD creation was in progress, then the process could be interrupted in the background. This will result in incomplete RRDs with missing information for logging and graphing of traffic and drops.

In later FortiDDoS-F-Series releases, the SPPs and RRDs for all possible SPPs are created during the upgrade process. However, existing incomplete RRDs will not be repaired. Checks of RRDs and SPPs are required if you are upgrading from 6.1.0, 6.1.4 or 6.2.0.

What's new

FortiDDoS-F 6.3.5 is a patch release, where no new features and enhancements are covered in this release. See Known issues on page 11 and Resolved issues on page 9 for details.

Hardware and VM support

FortiDDoS 6.3.5 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F
- FortiDDoS 2000F

FortiDDoS 6.3.5 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS 6.3.5 is NOT compatible with FortiDDoS-3000F.

FortiDDoS Release 6.3.5 supports deployment of FortiDDoS-VM in the following virtual machine environments:

- VMware
- KVM

Note: FortiDDoS VMs are not suitable for deployments in public cloud environments such as AWS, Azure or Google Cloud. The firmware will “work” but since FortiDDoS has no IP addresses on its data ports, there is no way to direct traffic to or through it. FortiDDoS must be installed on physical links.

Resolved issues

There are no firmware bug fixes in this release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Common Vulnerabilities and Exposures

For more information, visit https://www.fortiguard.com/psirt.

Bug ID	Description
790805	FortiDDoS-F 6.3.5 is no longer vulnerable to CVE-2022-27486.

Known issues

This section lists the known issues in FortiDDoS-F 6.3.5 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0765443	FortiDDoS will drop segmented/fragmented HTTP packets if HTTP Profile > Version Anomaly is enabled. **Do not enable** HTTP Version Anomaly. GET Cookies can be very large and frequently result in segmented HTTP packets. Trust the Method Thresholds to find HTTP attacks.
0794869	If multiple feature/Profile changes are made in an SPP, the Event Logs are concatenated and become difficult to understand.
0795300	DNS Dynamic Update Queries will be dropped by DNS Query Anomaly: Query Bit Set and DNS Response Anomaly: Query Bit not Set. Enterprise user should never see Dynamic Update Queries since they are normally used by services that host large numbers of different customer domains. If in doubt, disable these 2 DNS Anomalies.
0796137	On some graphs, when no drop count has been shown for a long time, if drops occur the system writes the graph backwards to the previous event, showing drops continuously when none actually happened (the logs are correct).
0668077	Local and External Authentication (RADIUS, LDAP, TACACS+) does not support 2-Factor Authentication.
0780476	In HA pairs, if a Primary system SPP is factory reset, the Secondary may not (reboot and) sync immediately.
0678434/0678433	FortiDDoS-F 6.1.x, 6.2.x and 6.3.x do not support LDAPS/STARTTLS.
0779671	HA Secondary systems do not create event logs for local events, such as logins.
0693789	When FDD-VM is operating on a virtual machine with underlying hardware supporting SR-IOV, disabling ports leads to unexpected results.
0785818	In Debug download > Customer Folder, the Attack log CSV does not always parse the attack log detail into correct columns.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0764676	`formatlogdisk` command from console does not show any output - only seen in (SSH) CLI.
0686846	Online SCEP Enrollment Method of Certificate generation fails.

Bug ID	Description
0638555/0637835/0634481/0633151	Multiple Queries in a single TCP DNS session (SourceIP:Port-DestinationIP:53) are allowed to exceed TCP DNS Thresholds. Fortinet's experience is that this is a very rare possibility. To work around, setting **DNS Anomaly Feature Controls: Query Anomaly: QDCount not One in Query** will drop these Queries as anomalies.
0714534	If setting Private Key and Certificate from CLI, the event log creates a blank message. Use GUI.
0695645	Under rare conditions, generating multiple Certificates after a configuration restore can stop the GUI.
0750762	FortiDDoS VMs support 1024 URL Hash Indexes while others support 64,000. This is by design.
0801480	When a new SPP is created and immediately sees traffic, it may take 10 minutes (2x 5-minute cycles) before drops and other information is shown. This is architectural and will not be changed.
0783004	FQDNs with TTLs longer than 30 days will create invalid entries in the Cache.
0795435	If DNS attack traffic is very bursty (short duration and infrequent) attack logs are correct but drop graphs may not show any information.

Upgrade notes

On the VM platform, to avoid the VMware network broadcast storm for the new deployment, each WAN/LAN interface pair is disabled by default so that traffic will not pass through.

In the initial deployment, please remember to enable the WAN/LAN interface pair via CLI.

```
# config system l2-interface-pair
# edit l2-port1-port2
# set status enable
# next
# end
```

Upgrading to 6.3.3 causes a 15s network outage, even if FortiDDoS Fail-Open is selected for appropriate traffic ports.

To avoid this, manually enter bypass before the upgrade

```
#: execute bypass-traffic enable
```

Select "y" at the prompt

Proceed with upgrade.

The bypass will be removed automatically when the system has rebooted and is operational.

After upgrade

Check the integrity of the system Service Protection Policies (SPPs) using the following CLI commands.

```
diagnose debug rrd_files_check
```

Output:

`Global expected:5, found:5` (this is the global SPP)

`SPP:0 expected:1857, found:1857` (this SPP is used internally)

`SPP:1 expected:1857, found:1857` (this is the default SPP)

`SPP:2 expected:1857, found:1857`

`SPP:3 expected:1857, found:1857`

`SPP:4 expected:1857, found:1857` (Limit for VM-04)

`SPP:5 expected:1857, found:1857`

`SPP:6 expected:1857, found:1857`

`SPP:7 expected:1857, found:1857`

`SPP:8 expected:1857, found:1857` (Limit for 200F/VM08)

`SPP:9 expected:1857, found:1857`

```
SPP:10 expected:1857, found:1857
SPP:11 expected:1857, found:1857
SPP:12 expected:1857, found:1857
SPP:13 expected:1857, found:1857
SPP:14 expected:1857, found:1857
SPP:15 expected:1857, found:1857
SPP:16 expected:1857, found:1857
```
(Limit for 1500F/2000F/VM16)

If the expected and found numbers above do not match (they may not be 1857 as above, but must match), you must follow the directions below to recreate/reset the RRDs.

Recreating/resetting the SPP RRDs removes all previous traffic and drop graphing information for that SPP. However, Logs are retained. If you are unsure on how to proceed, contact FortiCare for support.

Repair the SPP using the following CLI commands.

If SPP-0 is missing or missing RRDs:

```
execute backup-rrd-reset
```

It is important to repair this SPP-0 RRD first if the expected/found numbers do not match. This SPP is used to re-build SPPs 1-4/8/16.

If one or a few SPPs from 1-4/8/16 are missing RRDs:

`execute spp-rrd-reset spp <rule_name>` (where rule_name is the textual name from the GUI)

If many SPPs are missing RRDs:

```
execute rrd-reset all
```

If Global is missing RRDs:

```
execute global-rrd-reset
```

www.fortinet.com