FORTINET

Release Notes

FortiDDoS-F 6.2.3

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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 17, 2023
FortiDDoS-F 6.2.3 Release Notes
00-620-730305-20230317

TABLE OF CONTENTS

Change Log

Date	Change Description
March 17, 2023	FortiDDoS-F 6.2.3 Release Notes initial release

Introduction

This Release Notes covers the new features, enhancements, resolved issues and known issues of FortiDDoS version 6.2.3 build 0230.

Release 6.2.3 is provided primarily to back-port CVE fixes for customers still using Release 6.2.x. Fortinet **strongly recommends** upgrading to the latest FortiDDoS-F release to take advantage of all bug fixes and new features.

FortiDDoS F-series features a clean-sheet new architecture that draws on more than 10 years of FortiDDoS' DDoS mitigation experience while providing a flexible and forward-looking solution to detect and mitigate Layer 3 to Layer 7 DDoS attacks for enterprise data centers. FortiDDoS uses machine learning and behavior based methods, and monitors hundreds of thousands of networking parameters to build an adaptive baseline of normal activity. It then monitors traffic against that baseline and defends against every DDoS attack.

For those familiar with FortiDDoS B- and S-Series, FortiDDoS F-series 6.2.3 offers additional features, some changed functionality and some features that have been removed. A reference table is included for comparison.

After upgrading from 6.1.0, 6.1.4 or 6.2.x to FortiDDoS-F 6.2.3, please check the integrity of the system Service Protection Policies (SPPs) and repair if necessary. See After upgrade on page 10 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 6.2.3 is a patch release in which no new features and enhancements are covered in this release. See Known issues on page 9 and Resolved issues on page 8 for details.

Hardware and VM support

FortiDDoS 6.2.3 supports the following hardware models:

- FortiDDoS 200F
- FortiDDoS 1500F

FortiDDoS 6.2.3 is NOT compatible with any FortiDDoS A- / B- / E-Series hardware.

FortiDDoS Release 6.2.3 supports deployment of FortiDDoS-VM in the following virtual machine environments:

- VMware
- KVM

Resolved issues

The following issues have been resolved in the FortiDDoS-F 6.2.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0832996	HTTP GET/Post validation caused the VPP to restart which in turn toggled NICs, affecting traffic.
0852363	High speed, random Source IP and Port packets to TCP Port 80 can cause the HTTP GET/POST Mitigation to force a Virtual Packet Processor to restart, causing NIC flaps.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0839826	FortiDDoS-F6.2.3 is no longer vulnerable to the following CVE-Reference: CVE-2022-40679.
0790805	FortiDDoS-F6.2.3 is no longer vulnerable to the following CVE-Reference: CVE-2022-27486.
0776312	FortiDDoS-F6.2.3 is no longer vulnerable to the following CVE-Reference: CWE-121.
0772198	FortiDDoS-F6.2.3 is no longer vulnerable to the following CVE-Reference: CVE-2021-36173.
0772170	FortiDDoS-F6.2.3 is no longer vulnerable to the following CVE-Reference: CVE-2021-42757.

Known issues

This section lists the known issues in FortiDDoS-F 6.2.3 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0750762	FortiDDoS VMs support 1024 URL Hash Indexes while other models support 64,000. This is by design.
0714534	If setting Private Key and Certfiicate from CLI, the event log creates a blank message. Use GUI instead.
0695645	Under rare conditions, generating multiple Certificates after a configuration restore can stop the GUI.
0693789	When FDD-VM is operating on a virtual machine and underlying hardware supporting supporting SR-IOV, disabling ports leads to unexpected results.
0686846	Online SCEP Enrollment Method of Certificate generation fails.
0678445	Purging a large number of ACLs from an SPP can take more than 30 seconds with no progress indication.
0678434/0678433	Release 6.1.x and 6.2.x do not support LDAPS/STARTTLS.
0676634	GUI will allow multiple and overlapping Hash entries of various HTTP Thresholds like URL, Host, etc. Use care when manually entering indexes.
0672585	Very small, invalid DNS packets may be dropped even when no DNS Anomalies are enabled with no logging.
0671973	Global Service ACL explicitly for SCTP may have shown on earlier releases. This has not been implemented. Use Protocol # 132.
0668077	External Authentication (RADIUS, LDAP, TACACS+) does not support 2-factor authentication.
0637835/0638555	If multiple Questions are sent in the same TCP Query session where QD Count not equal to 1 is not enabled, the system will ignore the TCP Query Threshold. **Workaround**: Use the QD Count not equal to 1 anomaly. No DNS server will respond to two simultaneous Questions in one Query.
0630479	If multiple changes are made on a GUI page before saving, an event log is created for only one of the changes.
0626478	Trusted Hosts are not checked if LDAP/RADIUS/TACACS+ external authentication is used. Release 6.1.x and 6.2.0 do not support Trusted Hosts for LDAP / RADIUS / TACACS+.

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
```

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/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 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
```

Note: `All` is case-sensitive.

If `Global` is missing RRDs:

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

If any SPP is missing, contact FortiCare for support.

www.fortinet.com