Release Notes

FortiDeceptor 4.2.0

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/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

March 09, 2023
FortiDeceptor 4.2.0 Release Notes
50-420-801592-20230309

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-04-28	Initial release.
2023-03-09	Updated Resolved issues on page 10.

FortiDeceptor 4.2.0 release

This document provides information about FortiDeceptor version 4.2.0 build 0226.

Supported models

FortiDeceptor version 4.2.0 supports the following models:

FortiDeceptor	FDC-1000G
FortiDeceptor VM	FDC-VM (VMware ESXi, KVM, Hyper-V, AWS, GCP, and Azure)

What's new in FortiDeceptor 4.2.0

The following is a list of new features and enhancements in 4.2.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

Network Asset Discovery Module:

The new asset discovery generates the network asset inventory using passive network sniffing for network threat visibility and decoy deployment automation.

The network asset discovery supports both IT and IoT/OT networks.

Incident Alerts Reporting:

FortiDeceptor incident alert menu allows you to generate a new security report in PDF format from the incident alerts.

The PDF report style is similar to the FortiDeceptor report in FortiAnalyzer.

New Infrastructure Decoys:

FortiDeceptor expands the virtual appliance offering and now supports Hyper-V infrastructure.

New IT & Services Decoys:

IT Sensitive applications are always targets for threat actors and APT. Deception application Decoys are a key component for detecting attacks against critical applications. The following new Application Decoys were added:

- **ESXi Decoy:**
  - As part of the last attacks against VMware platform has a new ESXi Decoy.
  - The ESXi decoy is based on FortiDeceptor emulation technology

- **ELK (elastic search) Decoy:**
  - ELK has become one of the most popular data lake platform and also a target for data exfiltration attacks.
  - The ELK (elastic search) decoy is based on FortiDeceptor emulation technology.
- **New FTP service for windows & Linux Decoys:**
  - FTP service in enterprise network are used to host organization files.
  - The new FTP lure allows full customization of the service including anonymous access enablement, FTP credentials and FTP banner.

New Medical IoT Decoys:

- **New Medical IoT decoys:**
  - Expands the Medical decoy and adds Braun Infusomat pump.
  - Many vulnerabilities discovered in the Braun Infusomat pump product that exits widely in healthcare organization and become a target for threat actors.

New Deception Tokens Module:

The deception token package allows you to add breadcrumbs on real endpoints and deceive an attacker into a network Decoy. Deception Tokens are normally distributed within real endpoints and other IT assets on the network to maximize the deception surface

The new Deception token module allows you to generate a custom token campaigns from several decoys.

The new token campaigns support 2 deployment modes:

- **Online mode:**
  - The online deployment mode push the deception token dynamically based on the server side configuration.
  - The deception token package runs without token configuration and each token deployment. The endpoint retrieves the latest token configuration from the FDC manager.
  - This method allows the security team to change the deception campaign strategy dynamically and be more proactive against dynamic threats.
  - This method also allows the endpoint to report deployment status to the FortiDeceptor manager and provide real time visibility on the deception token deployment coverage.
- **Offline mode:**
  - The offline deployment mode generates a full deception token package with the token configuration embedded.

New Fabric Integrations:

- **MS ATP EDR**: Adds integration between FortiDeceptor and MS ATP EDR, allowing a threat mitigation response automation to isolate an infected machine from the network.
- **CrowdStrike EDR**: Adds integration between FortiDeceptor and CrowdStrike EDR, allowing a threat mitigation response automation to isolate an infected machine from the network.
- **Cuckoo Sandbox**: The integration between FortiDeceptor and Cuckoo Sandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.
- **FDC integration connector** works with FortiSIEM to update the “watch list” with deception credentials that were deployed in real time. The integration also automatically identify if a threat actor uses them across the network by checking the FSM logs in real time

Layer 2 Attacks:

MITM attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers.

FortiDeceptor expands the layer2 attacks detection by detecting ARP poising attack against real assets inside the same network VLANs where decoys are deployed.

Threat Intelligence Sharing:

The *IOC Export* page allows you to export the IOC file in CSV format and we have expanded it to allow pushing it automatically using STIX/TAXII protocol for a specified period.

The IOC file contains the Timestamp, Incident time, Attacker IP, related files, and WCF (Web Content Filtering) events.

You can also include MD5 checksums, WCF category, and reconnaissance alerts allowing Third-party Threat Intelligence Platforms to process the IOC data.

General:

- FortiDeceptor deployment wizard allows you to configure 2 DNS server per decoy.
- FortiDeceptor manager expands the user access authentication and now supports 2 FA authentication for radius. (for example, FortiToken).

Installation and upgrade

Installation information

For information about initial setup of FortiDeceptor on the FortiDeceptor 1000G model, see the *FortiDeceptor 1000G QuickStart Guide*.

For information about installing FortiDeceptor VM models, see the *FortiDeceptor VM Install Guide*.

All guides are available in the Fortinet Document Library.

Upgrade information

Download the latest version of FortiDeceptor from the Fortinet Customer Service & Support portal.

To upgrade the FortiDeceptor firmware:

1. Go to *Dashboard* > *System Information* > *Firmware Version*.
2. Click *[Update]*.
3. Select *Choose File*, locate the firmware image on your management computer.
4. Click *Submit* to start the upgrade.

Updating the FortiDeceptor firmware will not update the existing VM Images. However, it will re-initialize the existing Deception VMs to include bug fixes and enhancements.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Fortinet Customer Service & Support portal located at https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select Get Checksum Code.

Product integration and support

FortiDeceptor 4.2.0 support

The following table lists FortiDeceptor 4.2.0 product integration and support information:

Web Browsers	• Microsoft Edge version 42 and later • Mozilla Firefox version 61 and later • Google Chrome version 59 and later • Opera version 54 and later • Other web browsers may function correctly but are not supported by Fortinet.
Virtualization Environment	• VMware ESXi 5.1, 5.5, 6.0, 6.5, and 6.7. • KVM • AWS • GCP • Azure • Hyper-V
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 4.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
778027	NFR: Support the HyperV virtual platform for FDC VM model.
771791	NFR: Support New Deception Token Module.
778998	NFR: Prepare new deception OS base image Ubuntu16v2.
771786	NFR: Support FTP service on Linux and Windows decoys.
771793	NFR: FortiSIEM Watch-List Integration and Alerts Reporting.
771800	NFR: Fabric Integration with CrowdStrike isolation.
771806	NFR: Support Attacker IP-DNS Resolving.
771812	NFR: Support ARP Poisoning attacks detection.
771796	NFR: Fabric Integration with Cuckoo Malware Sandbox.
771805	NFR: Support STIX/TAXII / MISP TI Connector.
759738	NFR: Support 2 DNS IP in decoy.
763249	NFR: Provide GUI page to input the activation ID instead of `dcvm-confirm-id` CLI.
774445	NFR: Implement HTTP/HTTPS proxy support for web filter.
771776	NFR: Asset Discovery stage 1 - Passive OS fingerprint.
771779	NFR: Support ESXi Decoy.
771785	NFR: Support medical BBraun Infusomat Space Decoy.
771789	NFR: Support Elasticsearch service decoy.
771803	NFR: Fabric Integration with MS ATP Manager.
773486	NFR: Improve the PDF report with similar structure as FAZ deception incidents report.
722102	NFR: Inspect the related traffic only for incident to save HDD when there is a high volume traffic.
759090	NFR: Support automated un-installation process into Token installation for domain ENV.
795293	NFR: Support for creating Incident reports.
682479	NFR: Support 2 FA authentication for radius.

Bug ID	Description
789797	CSS: Custom SMB share folders to different groups in Custom Windows Image should not be ignored.
771675	CSS: The email alert attached to all the events information in HTML format as attachments which should be in email body.
777413	CSS: Issues with PAN Integration.
798135	FortiDeceptor - FortiSandbox / FortiDeceptor - No profile-based access control over APIs.
775218	Install ubuntu token failed for permission denied.
803008	Cloud client: Login page crashed in brand new Azure clients.
785637	Cloud client: Login page crashed in brand new GCP clients.
794879	Administrative access should only be enabled on Port1.
771670	Only the HDD file system error should be reported.
773478	Email rules should allow user to choose multiple severity levels.
797106	Display license expiry date in license page.
777864	Outgoing traffic from windows decoys.
777923	Improve time stamp convert function to reduce time.
788930	Email alert customer issues.
779644	HTTP OPTIONS requests are being made to network shares and are being logged as medium risk incidents.
779634	Decoy status page: Hide the password for domain in *Network* section.
800480	TP LINK router: TP LINK Web Postman access failed.
779642	Support upper case for SMB share name for windows decoys.
777528	Custom Windows 2019: Missing SMB events.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
798135	FortiDeceptor 4.2.0 is no longer vulnerable to the following CVE: • CVE-2022-27487

Known issues

The following issues have been identified in version 4.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
768406	NFR: FDC conserve mode when disk usage above threshold.
758384	Firmware upgrade needs confirmation from user and show some response.
802602	Honeydoc needs to support HTTPS.
765907	Hint message for DMZ mode should also apply to CM Manager when Client is in DMZ mode.
766605	CLI improvement under CM Manager mode.
791811	2FA login will fail if FAC radius policy enable OTP only mode.
793993	Allow edit of monitor network config when used by decoy.
779317	Packets are dropped by OVS bridge sometimes.
779645	Improve the HTTP *request/response* in the *Incident* page.
770368	Deployment Wizard: SAP DISPATCHER user input has no max length limitation.
763034	Logging out does not clear saved Attack Map.
714282	SYSTEM: Admin Profiles cannot create new admin profile to let some administrators to create/edit/delete normal users.
767082	Incident CSV export needs improvement.

www.fortinet.com