NetWitness® Platform XDR

Version 11.7.2.0

Release Notes

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

December, 2022

Contents

What's New

The NetWitness Platform XDR 11.7.2.0 release provides new features and enhancements for every role in the Security Operations Center.

Security Fixes

This service pack release of NetWitness Platform XDR addresses the following vulnerabilities:

- CVE-2022-2526
- CVE-2022-21123
- CVE-2022-21125
- CVE-2022-21166
- CVE-2022-21618
- CVE-2022-21619
- CVE-2022-21624
- CVE-2022-21626
- CVE-2022-21628
- CVE-2022-29154
- CVE-2022-38177
- CVE-2022-38178
- CVE-2022-39399
- CVE-2022-40674

For more information on the various vulnerabilities fixed in this service pack release, see https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security

Note: If you have the Export Connector plugin in your deployment, you must do the following:
- If you have Logstash installed separately, not as part of the NetWitness installation, you must uninstall the Export Connector plugin and install the updated Export Connector plugin after 11.7.2 patch upgrade. For more information to install the updated plugin, see *Post-Upgrade Tasks* on the Upgrade Guide for 11.7.2
- If you have Logstash installed as part of the NetWitness installation on the Log Collector service, the updated Export Connector plugin will be automatically installed during the 11.7.2 patch upgrade.

In both the above cases, the old Export Connector plugin files are not automatically removed after upgrade. You must remove the old plugin files, so the scans do not list them as vulnerabilities. For more information on how to remove the old plugin files, see see *Post-Upgrade Tasks* on the Upgrade Guide for 11.7.2

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform XDR 11.7.2.0:

- NetWitness Platform XDR 11.5.3.2 to 11.7.2.0
- NetWitness Platform XDR 11.5.3.3 to 11.7.2.0
- NetWitness Platform XDR 11.6.0.0 to 11.7.2.0
- NetWitness Platform XDR 11.6.1.0 to 11.7.2.0
- NetWitness Platform XDR 11.6.1.1 to 11.7.2.0
- NetWitness Platform XDR 11.6.1.2 to 11.7.2.0
- NetWitness Platform XDR 11.6.1.3 to 11.7.2.0
- NetWitness Platform XDR 11.6.1.4 to 11.7.2.0
- NetWitness Platform XDR 11.7.0.0 to 11.7.2.0
- NetWitness Platform XDR 11.7.0.1 to 11.7.2.0
- NetWitness Platform XDR 11.7.0.2 to 11.7.2.0
- NetWitness Platform XDR 11.7.1.0 to 11.7.2.0
- NetWitness Platform XDR 11.7.1.1 to 11.7.2.0
- NetWitness Platform XDR 11.7.1.2 to 11.7.2.0

For more information on upgrading to 11.7.2.0, see Upgrade Guide for NetWitness Platform XDR 11.7.2.0

Fixed Issues

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the NetWitness Platform XDR Known Issues list on NetWitness Platform XDR Community portal.

Log Collection Fixes

Tracking number	Description
ASOC-123921	After upgrading to 11.7.1.0, WinRM log collection is interrupted due to the conflict in the internal artifact. As a result, logs are not collected from the WinRM server.

ESM Fixes

Tracking number	Description
ASOC-117261	The parser mapping (**Event Source Monitoring** > **Discovery**) is not working, and it reverts to 'None' due to **Acknowledge** tab reverting to **NO** in every 10 minutes.

Health & Wellness Fixes

Tracking number	Description
ASOC-122365	The Hosts section under **Health & Wellness** > **Monitoring** doesn't display the **Physical drive**, **logical drive**, and **adapter** details due to an upgrade of the perccli library to the newer version.

Core services (Broker, Concentrator, Decoder, Archiver) Fixes

Tracking number	Description
ASCO-123701	In Events or Investigate section, if parsing any packets of any conversations involving an attachment of MSI type, then it is displayed and gets downloaded as a .docx file.
ASOC-123676	Decoder packet pool gets depleted while parsing HTTP2 session because while parsing HTTP2 headers, Decoder process sometimes hangs when an overly long literal value is present in HTTP2 headers.

Security Fixes

Tracking number	Description
ASOC - 121942	Security scanner reported that **HSTS Security Header** (Strict-Transport-Security parameter) missing from **HTTPS Response Header** on NextGen Core Service Rest Ports/Pages.

Respond Fixes

Tracking number	Description
ASOC-123712	Naming pattern issue was observed after upgrading to 11.7.1.1, and because of that, it was not possible to open an incident in UI. Curly brackets or braces in Alert and Incident rule in Respond being unable to link back to the original event.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform XDR 11.x Master Table of Contents	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform XDR 11.7 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform XDR 11.7 Upgrade Guide	https://community.netwitness.com/t5/netwitness-platform-online/upgrade-guide-for-11-7/ta-p/652427

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform XDR documentation.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness Platform XDR:

- See the documentation for all aspects of NetWitness Platform XDR here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Create a Post** fields in NetWitness Platform XDR Community portal to find specific information here:https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- See the NetWitness Platform XDR Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Platform XDR Support

If you contact NetWitness Platform XDR Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the NetWitness Platform XDR product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

NetWitness Platform XDR Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Platform XDR Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform XDR 11.7.2.0.

Component	Version Number
NetWitness Audit Plugins	rsa-audit-plugins-11.7.2.0-4786.5.5e85c080e.el7.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-11.7.2.0-4786.5.5e85c080e.el7.x86_64.rpm
NetWitness Admin Server	rsa-nw-admin-server-11.7.2.0-221205025753.5.52e581e.el7.centos.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-11.7.2.0-2209300528.5.24cc6a9.el7.noarch.rpm
NetWitness Broker	rsa-nw-broker-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-11.7.2.0-2688.5.46edb4e56.el7.x86_64.rpm
NetWitness Cloud Link Server	rsa-nw-cloud-link-server-11.7.2.0-221205051934.5.73980af.el7.centos.noarch.rpm
NetWitness Collectd	rsa-collectd-11.7.2.0-4786.5.5e85c080e.el7.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-11.7.2.0-4786.5.5e85c080e.el7.x86_64.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-11.7.2.0-2212082154.5.ebdf3f4.el7.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-11.7.2.0-2209300538.5.ec64d8e.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-11.7.2.0-221205040506.5.b0f170b.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-11.7.2.0-221202062729.5.94f374f.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-11.7.2.0-221202064714.5.5c70b89.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-11.7.2.0-221206103612.5.0acfb30.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm

NetWitness Decoder Content	rsa-nw-decodercontent-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-11.7.2.0-2209300539.5.efe4c2d.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-11.7.2.0-2210190934.5.276c329.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.7.2.0-221205045746.5.f2b2f43.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-11.7.2.0-221205054959.5.c44e53a.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-11.7.2.0-221205040946.5.de1fcad.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-11.7.2.0-221206001237.5.1b2c444.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-11.7.2.0-221202171458.5.2afa9b0.el7.centos.noarch.rpm
NetWitness License Server	rsa-nw-license-server-11.7.2.0-221205033325.5.068d944.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-11.7.2.0-15013.5.9fca292a3.el7.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-11.7.2.0-15013.5.9fca292a3.el7.x86_64.rpm
NetWitness Log Collector Tools	rsa-nw-logcollector-tools-11.7.2.0-15013.5.9fca292a3.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-11.7.2.0-221010105350.5.f31692f.el7.centos.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-11.7.2.0-221202060519.5.aa044a7.el7.centos.noarch.rpm
NetWitness Orchestration CLI	rsa-nw-orchestration-cli-11.7.2.0-2212050526.5.b3b43ab.el7.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-11.7.2.0-221202073740.5.0e80a0f.el7.centos.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm

NetWitness Presidio Core	rsa-nw-presidio-core-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm
NetWitness Presidio Elastic Search Initiation	rsa-nw-presidio-elasticsearch-init-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm
NetWitness Presidio Ext	rsa-nw-presidio-ext-netwitness-11.7.2.0-2212021720.5.61f6f1a.el7.noarch.rpm
NetWitness Presidio Flume	rsa-nw-presidio-flume-11.7.2.0-2212021719.5.6bacec4.el7.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-11.7.2.0-2212021708.5.c61002a.el7.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-11.7.2.0-2212021722.5.8ede162.el7.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-11.7.2.0-5926.5.a6cd2d42a.el7.x86_64.rpm
NetWitness Recovery Tool	rsa-nw-recovery-tool-11.7.2.0-2210271105.5.f31fc03.el7.noarch.rpm
NetWitness Relay Server	rsa-nw-relay-server-11.7.2.0-221205045842.5.c42e97b.el7.centos.noarch.rpm
NetWitness Respond Server	rsa-nw-respond-server-11.7.2.0-221206003229.5.041f221.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-11.7.2.0-2212050641.5.d9a9fb4.el7.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-11.7.2.0-2209300539.5.298be30.el7.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-11.7.2.0-4786.5.5e85c080e.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-11.7.2.0-4786.5.5e85c080e.el7.x86_64.rpm
NetWitness Security CLI	rsa-nw-security-cli-11.7.2.0-2212050725.5.dde1dd3.el7.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-11.7.2.0-221205033146.5.53afa1b.el7.centos.noarch.rpm
NetWitness Shell	rsa-nw-shell-11.7.2.0-221202042748.5.082403d.el7.centos.noarch.rpm
NetWitness Source Server	rsa-nw-source-server-11.7.2.0-221205111714.5.0078e2d.el7.centos.noarch.rpm
NetWitness User Interface	rsa-nw-ui-11.7.2.0-221019000447.5.81152b17fd.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-11.7.2.0-12283.5.bbec02093.el7.x86_64.rpm

Revision History

Date	Description
December 2022	General Availability