Sensus Approved Updates

November 4, 2024

The following updates were released by Red Hat for Enterprise Linux 6, 7, and 8 environments in October 2024. Sensus has reviewed these updates and applied them to our Development and Quality Assurance environments.

For additional information and updates please visit https://www.xylem.com/en-us/about-xylem/cybersecurity/sensus-product-security/

Red Hat Enterprise Linux 6

There were no applicable updates to RHEL6 in October 2024.

Red Hat Enterprise Linux 7

The following updates were verified for basic functionalities of the NA 4.13 release. Sensus expects these updates to be applicable to earlier releases stated in the table below. Please review the below updates for installation in your environment. Sensus recommends applying any changes to a Test/Quality Assurance environment before releasing to a production environment.

Date	Type	Advisory	Synopsis	RNI Release
2024-10-07	security	RHSA-2024:7705	Moderate: systemd security update	v4.1 - v4.13
2024-10-16	security	RHSA-2024:8120	Moderate: java-11-openjdk security update	v4.11 - v4.13
2024-10-23	security	RHSA-2024:8365	Moderate: python-idna security update	v4.1 - v4.13
2024-10-28	security	RHSA-2024:8495	Important: postgresql security update	v4.1 - v4.13

Red Hat Enterprise Linux 8

RNI

The following updates were verified for basic functionalities of the NA 4.15 release. Sensus expects these updates to be applicable to earlier releases stated in the table below. Please review the below updates for installation in your environment. Sensus recommends applying any changes to a Test/Quality Assurance environment before releasing to a production environment.

Date	Type	Advisory	Synopsis	RNI Release
2024-10-01	security	RHSA-2024:7481	Important: linux-firmware security update	v4.14,v4.15,CB7.0.2
2024-10-09	security	RHSA-2024:7848	Low: openssl security update	v4.14,v4.15,CB7.0.2
2024-10-13	security	RHSA-2024:8038	Important: container-tools:rhel8 security update	v4.14,v4.15,CB7.0.2
2024-10-15	enhancement	RHEA-2024:8159	microcode_ctl bug fix and enhancement update	v4.14,v4.15,CB7.0.2
2024-10-16	security	RHSA-2024:8124	Moderate: java-17-openjdk security update	V4.15,CB 7.0.2
2024-10-22	security	RHSA-2024:8327	Important: grafana security update	v4.14,v4.15,CB7.0.2
2024-10-23	security	RHSA-2024:8353	Important: NetworkManager-libreswan security update	v4.14,v4.15,CB7.0.2

NCS

The following updates were verified for basic functionalities of the NCS 2.1.2 release. Sensus expects these updates to be applicable to earlier releases stated in the table below. Please review the below updates for installation in your environment. Sensus recommends applying any changes to a Test/Quality Assurance environment before releasing to a production environment.

Date	Type	Advisory	Synopsis	RNI Release
2024-10-01	security	RHSA-2024:7481	Important: linux-firmware security update	NCS 2.1.2
2024-10-09	security	RHSA-2024:7848	Low: openssl security update	NCS 2.1.2
2024-10-13	security	RHSA-2024:8038	Important: container-tools:rhel8 security update	NCS 2.1.2

Date	Type	Advisory	Synopsis	RNI Release
2024-10-15	enhancement	RHEA-2024:8159	microcode_ctl bug fix and enhancement update	NCS 2.1.2