

Sensus Approved Updates

December 1, 2025

The following updates were released by Red Hat for Enterprise Linux 7 and 8 environments in November 2025. 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 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
2025-11-06	security	RHSA-2025:19847	Important: sssd security update	v4.1 - v4.13
2025-11-12	security	RHSA-2025:21063	Moderate: kernel security update	v4.1 - v4.13
2025-11-17	security	RHSA-2025:21407	Important: libtiff security update	v4.1 - v4.13
2025-11-18	bugfix	RHBA-2025:21687	glib2 bug fix and enhancement update	v4.1 - v4.13
2025-11-18	security	RHSA-2025:21657	Important: libsoup security update	v4.1 - v4.13
2025-11-25	security	RHSA-2025:22040	Low: xorg-x11-server security update	v4.1 - v4.13

Red Hat Enterprise Linux 8

RNI

The following updates were verified for basic functionalities of the NA 4.16 and CB 7.3.0 releases. 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
2025-11-03	bugfix	RHBA-2025:19554	mdadm bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	bugfix	RHBA-2025:19555	microcode_ctl bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	bugfix	RHBA-2025:19556	systemd bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	bugfix	RHBA-2025:19557	glib2 bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	bugfix	RHBA-2025:19559	initscripts bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	bugfix	RHBA-2025:19576	plymouth bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-03	security	RHSA-2025:19447	Moderate: kernel security update	v4.14 - v4.16,CB7.3.0
2025-11-04	bugfix	RHBA-2025:19558	linux-firmware bug fix and enhancement update	v4.14 - v4.16,CB7.3.0
2025-11-04	bugfix	RHBA-2025:19569	samba bug fix and enhancement update	v4.14 - v4.16
2025-11-04	security	RHSA-2025:19610	Important: sssd security update	v4.14 - v4.16,CB7.3.0
2025-11-04	security	RHSA-2025:19714	Important: libsoup security update	v4.14 - v4.16,CB7.3.0
2025-11-05	security	RHSA-2025:19835	Important: bind security update	v4.14 - v4.16,CB7.3.0
2025-11-06	security	RHSA-2025:19909	Important: tigervnc security update	v4.14 - v4.16
2025-11-09	security	RHSA-2025:19931	Moderate: kernel security update	v4.14 - v4.16,CB7.3.0
2025-11-10	security	RHSA-2025:20034	Important: libtiff security update	v4.14 - v4.16,CB7.3.0

Date	Type	Advisory	Synopsis	RNI Release
2025-11-11	security	Security Update for SQL Server 2019 CU32 (KB5068404)	Security issues have been identified in the SQL Server 2019 RTM CU that could allow an attacker to compromise your system and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.	CB7.3.0
2025-11-16	security	RHSA-2025:21398	Moderate: kernel security update	v4.14 - v4.16,CB7.3.0
2025-11-19	security	RHSA-2025:21776	Important: expat security update	v4.14 - v4.16,CB7.3.0
2025-11-23	security	RHSA-2025:21917	Moderate: kernel security update	v4.14 - v4.16,CB7.3.0
2025-11-24	security	RHSA-2025:21977	Moderate: libssh security update	v4.14 - v4.16,CB7.3.0
2025-11-25	security	RHSA-2025:22063	Moderate: cups security update	v4.14 - v4.16,CB7.3.0

NCS

The following updates were verified for basic functionalities of the NCS 2.2.0 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	NCS Release
2025-11-03	bugfix	RHBA-2025:19554	mdadm bug fix and enhancement update	v2.2.0
2025-11-03	bugfix	RHBA-2025:19555	microcode_ctl bug fix and enhancement update	v2.2.0
2025-11-03	bugfix	RHBA-2025:19556	systemd bug fix and enhancement update	v2.2.0
2025-11-03	bugfix	RHBA-2025:19557	glib2 bug fix and enhancement update	v2.2.0

Date	Type	Advisory	Synopsis	NCS Release
2025-11-03	bugfix	RHBA-2025:19559	initscripts bug fix and enhancement update	v2.2.0
2025-11-03	bugfix	RHBA-2025:19576	plymouth bug fix and enhancement update	v2.2.0
2025-11-03	security	RHSA-2025:19447	Moderate: kernel security update	v2.2.0
2025-11-04	bugfix	RHBA-2025:19558	linux-firmware bug fix and enhancement update	v2.2.0
2025-11-04	security	RHSA-2025:19610	Important: sssd security update	v2.2.0
2025-11-05	security	RHSA-2025:19835	Important: bind security update	v2.2.0
2025-11-09	security	RHSA-2025:19931	Moderate: kernel security update	v2.2.0
2025-11-13	security	RHSA-2025:21232	Important: container-tools:rhel8 security update	v2.2.0
2025-11-16	security	RHSA-2025:21398	Moderate: kernel security update	v2.2.0
2025-11-19	security	RHSA-2025:21776	Important: expat security update	v2.2.0
2025-11-23	security	RHSA-2025:21917	Moderate: kernel security update	v2.2.0
2025-11-24	security	RHSA-2025:21977	Moderate: libssh security update	v2.2.0