October 17, 2023

Mandatory Action Required
Removal of CentOS and Red Hat Enterprise Linux (RHEL) 7

The U.S. Department of Health and Human Services (HHS) requires that when an operating system, software, or application is nearing the End of Life (EOL) based on vendor notifications or postings, the risk must be mitigated by either upgrading, retiring, or stopping the use of an unsupported operating system, software, or application.

CentOS

In 2020, The CentOS Project, in coordination with Red Hat, announced that it would shift full investment to CentOS Stream, the upstream development platform for upcoming Red Hat Enterprise Linux releases. As a result, CentOS Linux will reach the end of life (EOL) on June 30, 2024. If you are running CentOS Linux in the QualityNet environment, you are asked to **migrate** to a new operating system, such as Red Hat Enterprise Linux (RHEL) or Amazon Linux 2, **before December 31, 2023**.

We strongly encourage all users to take the necessary steps to migrate their applications in a timely manner to avoid any potential disruptions. CentOS must be fully removed from QualityNet. This requires Application Development Organizations (ADOs) to stop usage and remove "stopped" instances in their AWS accounts. A "stopped" instance must be terminated to be fully removed from the environment.

RHEL 7

Red Hat Enterprise Linux (RHEL) 7 will stop all maintenance support from the vendor on June 30, 2024. The last minor release of RHEL 7 is 7.9, which will also be supported until June 30, 2024.

Due to critical vulnerabilities in RHEL 7 that will not be addressed by the vendor, and to align with HHS and Centers for Medicare & Medicaid Services (CMS) Acceptable Risks Safeguards (ARS) – SA-22 (Unsupported System Components), all Application Development Organizations (ADOs) are required to commence decommissioning efforts to **transition away from RHEL 7 immediately**.

ADOs must replace or upgrade system components related to RHEL 7 by **no later than March 1, 2024**.

If the timelines for CentOS or RHEL 7 cannot be met, Business and System Owners must submit a formal Risk-Based Decision (RBD) for approval by the CMS Chief Information Security Officer (CISO) and Chief Information Officer (CIO). The RBD should include:

- A comparison of options for sustaining, upgrading, or replacing unsupported software.
- An explanation of compensating controls implemented to mitigate the risk associated with unsupported software.
- Confirmation of planned/allocated funding.
- A scheduled date for removing, retiring, or upgrading of unsupported software or applications.

If an RBD is rejected, all instances of CentOS or RHEL 7 must be removed from the network immediately or by the EOL date. Any new vulnerabilities that may emerge can lead to the rejection of previously approved risk acceptances or RBDs in accordance with Binding Operational Directive (BOD) 19-02.

Please ensure your system is in full compliance with these guidelines to uphold the security posture and policies set forth within HHS. If you have any questions or concerns, please contact your Information System Security Officer (ISSO) for additional information and guidance.

If you need additional information, please work with your assigned CMS Information System Security Officer (ISSO): List here , the HIDS Security Analyst team, or reach out on QualityNet Slack: #qnet-security-community.

Join the QualityNet Mailer List:
Qnet Security Communications

Center for Clinical Standards and Quality (CCSQ)