

Summary

This bulletin serves as a notice of several recently reported Common Vulnerabilities and Exposures (CVEs) in the Niagara Framework® and releases that address them. Corrections applied include but are not limited to:

- Ensuring that characters stored in some configuration files are properly escaped or rejected.
- Improvements to user permission validation during file writes.
- Updates to some cryptographic parameters to accommodate the latest recommendations.

CVE ID*
CVE-2025-3936
CVE-2025-3937
CVE-2025-3938
CVE-2025-3939
CVE-2025-3940
CVE-2025-3941
CVE-2025-3942
CVE-2025-3943
CVE-2025-3944
CVE-2025-3945
*CVE links may not be functional while CVE reporting is in progress.

Affected Products

The following is a list of affected products.

- Niagara Framework 4.10u10
- Niagara Framework 4.14u1
- Niagara Framework 4.15

Recommended Action

It is important that all Niagara customers for all supported platforms update their systems with these releases to mitigate risk. If you have any questions, please contact your KMC AVP or Customer Support at [KMC Customer Support](#). As always, we highly recommend that Niagara customers running on unsupported platforms (such as Niagara AX or older versions of Niagara 4) take action to update their systems to a supported platform.

The following releases of KMC Workbench contain patch fixes of the Niagara framework to address the CVEs noted above.

- 4.10u11
- 4.14u2
- 4.15u1

Mitigation

In addition to updating your system, it is recommended that customers take the following steps to protect themselves:

- Review and validate the list of users who are authorized and who can authenticate to Niagara.
- Allow only trained and trusted persons to have physical access to the system, including devices that have connection to the system through the Ethernet port.
- Consider using a VPN or other means to ensure secure remote connections into the network where the system is located if remote connections are enabled,
- Sign all modules and program objects provided by third-party teams.
- Review the [Niagara Hardening Guide](#) and implement the recommended techniques for securing your installation
- Review the Security Dashboard for current installations that may have any warnings or errors.