Update Your Niagara Software to Address Several Vulnerabilities Identified in the Niagara Framework ®

Security Bulletin #: SB 2025-Tridium-1
Defect#: PSIRT-1229

CVE ID	CVSS Vector	Score
CVE-2025-3936	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	6.5
CVE-2025-3937	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
CVE-2025-3938	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N	6.8
CVE-2025-3939	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3
CVE-2025-3940	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
CVE-2025-3941	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N	5.4
CVE-2025-3942	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
CVE-2025-3943	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N	4.1
CVE-2025-3944	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
CVE-2025-3945	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

NOTE: CVE links may not be functional while CVE reporting is in progress.

Summary

This bulletin is to make you aware of a few recently reported vulnerabilities. The fixes applied include but are not limited to:

- Properly escaping characters or rejecting characters stored in some configuration files.
- Improved user permission validation during file writes.
- Updated some cryptographic parameters to accommodate latest recommendations.

Affected Supported Products

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

Recommended Action

Tridium recommends upgrading to Niagara 4.14u2 and Niagara EntSec 4.14u2 for any Niagara 4.14 deployments. These updates are available by contacting your sales support channel or by contacting the Tridium support team at support@tridium.com.

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 Tridium account manager or Customer Support at support@tridium.com. As always, we highly recommend that Niagara customers running on unsupported platforms (such as Niagara AX) take action to update their systems to a supported platform.

NOTE: Updates to Niagara 4.10 and Niagara 4.15 will be released shortly.

Mitigation
In addition to updating your system, Tridium recommends that customers with affected products 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 though 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.

Cybersecurity is a priority at Tridium. We are dedicated to continuously improving the security of our products, and we will continue to update you as we release new security features, enhancements, and updates.

Acknowledgement
Tridium would like to acknowledge Andrea Palanca and team at Nozomi Networks for their help in identifying this set of vulnerabilities and reporting them to us.

Appendix
The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors. The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION IN THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- TRIDIUM RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- TRIDIUM PROVIDES THE CVSS SCORES 'AS IS' WITHOUT WARRANTY OF ANY KIND. TRIDIUM DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL TRIDIUM BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT. SPECIAL, OR CONSEQUENTIAL DAMAGES.

May 2025