

Security Bulletin

SecB0012: Niagara

Summary

First published: May 22, 2025

Description	Update Your Niagara Software to Address Several Vulnerabilities Identified in the Niagara Framework ®
Affected Products	Niagara Framework, Niagara Enterprise Security
Recommended Action	Please update any installations of Niagara 4.14 to Niagara 4.14U2 Updates for Niagara 4.10 and Niagara 4.15 will be released shortly.

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-2025-3944	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
CVE-2025-3945	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	4.7
CVE-2025-3945	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	4.7

Security Bulletin

Description

This bulletin is to make you aware of a few recently reported vulnerabilities within Niagara. 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.

Recommended Action

Please update any installations of Niagara 4.14 to Niagara 4.14U2

Updates for Niagara 4.10 and Niagara 4.15 will be released shortly.

Delta Controls branded builds of these Niagara framework software updates are available from [the Delta Controls Support site software downloads](#) page.

It is important that all Niagara customers for all supported platforms update their systems with these releases to mitigate risk.

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.

If you have any questions, please contact Customer Support via technicalsupport@deltaccontrols.com.

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.