

[View in Browser](#)

## Please Update Your Niagara Software to Address Program Module Vulnerability

**Security Bulletin #:** SB 2026-Tridium-1  
**Defect#:** PSIRT-1463

### CVE ID Score

CVE ID	CVSS Vector	Score
<a href="#">CVE-2026-11804</a>	AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N	5.2

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

### Summary

This bulletin is to make you aware of a privilege escalation vulnerability identified in the program module.

### Affected Supported Products

- Niagara Framework® 4.14u5
- Niagara Enterprise Security 4.14u5
- Niagara Framework 4.15u4
- Niagara Enterprise Security 4.15

### Recommended Action

Tridium recommends obtaining the patches below and applying them to any Niagara 4.14u5 systems and earlier.

- program-rt-4.14.5.22.1.jar
- program-rt-4.15.4.24.1.jar

Alternatively, the updates are available in the following Niagara versions:

- Niagara Framework 4.14u6
- Niagara Enterprise Security 4.14u6
- Niagara Framework 4.15u5
- Niagara Enterprise Security 4.15u5

These updates are available on the [Niagara Central](#) download site, by contacting your sales support channel, or by contacting the Tridium support team at [support@tridium.com](mailto: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](mailto: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.

## 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 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.

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 [Umut Pirkoca](#) for his help in identifying this vulnerability and reporting it 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.

July 2026

**DISCOVER. CONNECT. ACHIEVE**



**ABOUT US**

Tridium is a world leader in business application frameworks — advancing truly open environments that harness the power of the Internet of Things. Our products allow diverse monitoring, control and automation systems to communicate and collaborate in buildings, data centers, manufacturing systems, smart cities and more. We create smarter, safer and more efficient enterprises and communities — bringing intelligence and connectivity to the network edge and back.

[tridium.com](http://tridium.com)

[Privacy Statement](#)

© 2026 Tridium Inc.



If you no longer wish to receive these emails, you may unsubscribe here: [Unsubscribe](#)

Please do not ask to unsubscribe by email. This inbox is not monitored.