Security Advisory No. 003

Date: 12th Jan 2022

Improper authentication and path traversal vulnerabilities in third party Tridium Niagara platform

Advisory ID: PD-2022-001
Document Version: 1.0
First published: 2022-01-12
Last updated: N/A (Initial version)

Advisory Title

Improper authentication and path traversal vulnerabilities in third party Tridium Niagara platform.

Summary

Philips Dynalite is aware of vulnerabilities in the third party Tridium Niagara platform which is used in the DDNG-BACnet gateway and in Niagara SOFTJACE.

CVE-2017-16748 - An attacker can log into the local Niagara platform (Niagara AX Framework Versions 3.8 and prior or Niagara 4 Framework Versions 4.4 and prior) using a disabled account name and a blank password, granting the attacker administrator access to the Niagara system.

CVE-2017-16744 - A path traversal vulnerability in Tridium Niagara AX and Niagara 4 systems installed on Microsoft Windows Systems can be exploited by leveraging valid platform (administrator) credentials.

Affected Products

Product	Affected Versions	Remediation
DDNG-BACnet	Niagara N4 platform version before version 4.4.92.2	Update Niagara platform to 4.4.92.2.1 or newer
	Niagara AX platform up to version 3.8	Update Niagara platform to 3.8.401 or newer
SOFTJACE	Niagara N4 platform before version 4.4.92.2	Update Niagara platform to 4.4.92.2.1 or newer
	Niagara AX platform up to version 3.8	Update Niagara platform to 3.8.401 or newer

Details

The fix for the DDNG-BACnet will require the use of Tridium Niagara Workbench software to perform the upgrade/recommissioning of the JACE platform.

CVE-2017-16744 affects only SOFTJACE running on Microsoft Windows. It does not affect the DDNG-BACnet.

Obtaining Software Fixes

Niagara platform updates are available from Tridium.

Contact Philips Dynalite technical support if assistance is required.
https://www.dynalite.org/support

Mitigations and Workarounds

The following defensive measures are recommended to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods such as Virtual Private Networks (VPNs).

Vulnerability Classification

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

CVSS 3.x Severity and Metrics:

CVE-2017-16748
Base Score: 9.8 CRITICAL
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2017-16744
Base Score: 7.2 HIGH
Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Terms of Use

Signify Security Advisories are subject to the terms and conditions contained in Signify underlying license terms or other applicable agreements previously agreed to with Signify (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Signify Security Advisory, the Terms of Use of Signify Global
Website: https://www.signify.com/global/conditions-of-commercial-sale. In case of conflicts, the License Terms shall prevail over the Terms of Use.