Building Automation Systems - Cybersecurity Best Practices & Lessons Learned

June 24, 2020

Q&A

1. We are implementing multiple community / cloud-based Niagara implementation. Our Client has OKTA as the centralized authentication mechanism. The only users that will access the Niagara will be employees. We proposed to them to keep the entire system behind VPN. Client's request is to not have it behind VPN and just use OKTA authentication. What is Tridium's suggestion on this? We will be running Niagara 4.8 and they use OKTA for authentication. Could you provide clue as to how is VPN going to help over and above OKTA? We plan to do SSO with OKTA/Niagara SAML integration.

   We will try to answer question in a few parts:

   1. SAML Identity Provider(IDP) - We implemented SAML-based SSO according to the SAML 2.0 specification. We tested integration with a large amount of identity providers, but we are unaware of anyone integrating with OKTA at this point, and we have not tested integration with OKTA. We are assuming that Niagara will integrate well with OKTA, but haven't talked with an SI that has integrated with OKTA yet. We do want to mention that with Niagara 4.9, we are releasing a Niagara-based IDP for others who do not have access to an organizational SAML IDP
   2. A VPN provides confidentiality and integrity of all the data in transit, and provides protection against a number of different attacks. What is helpful about putting an entire system behind a VPN is that it blocks all Internet exposure to all the IP addresses and related traffic behind that VPN, and in addition, provides the protections listed earlier. While the IDP itself provides Single Sign-On (SSO), putting all systems behind a VPN complements that authentication feature with confidentiality and integrity of all systems.

2. Will you make available the CISA document?

   Yes – it will be in the presentation for the session, but you can also find it here: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

3. What version of N4 was the security dashboard released?

   Niagara 4.8

4. Is the security dashboard available in the standard libraries in the JACE and Niagara platform?

   It requires the nss module to be installed with 4.8 or newer version. The nss module must be installed on the Supervisor and all subordinate JACEs in order to communicate this data back to a dashboard that is hosted at the Supervisor.

5. Is a license required for the nss module?

   You should be able to update the license from the license server to pick up the nss feature for a supervisor to utilize the system wide dashboard view. The station dashboard view does not utilize a license feature.

6. What is the biggest vulnerability that people face with outdated Tridium systems? (port 1911? being exposed on shodan? bruteforce? ddos attacks?)

   This is a really good question. Your example of systems running port 1911 (insecure/unencrypted FOX) and being exposed on the Internet (and therefore on Shodan) is in the category of poor configuration. In exposing unencrypted/unprotected FOX, that is an example of a bad configuration of a Niagara system (either that – or it's an example of an incredibly old Niagara system where TLS was not there to protect the confidentiality and the integrity of traffic!)

   In the example of systems exposed on the Internet, this is not related to your version, but it is poor network setup and poor network configuration which could put your entire network at risk, because it is essentially an "advertisement" for hackers to try to attack. This is why we recommend setting up your network with a Defense-In-Depth strategy (paper recommended in the presentation) where you don't expose ANY of your systems to the Internet to be discovered. When you have a system (any system) exposed on the Internet, sites like Shodan and Censys make it easy for hackers to find your system. Once they find it, they will see if there are any published vulnerabilities or known exploits about the system, or they could simply try attacks on your system. Many of these attacks are easy and automated.

   In order to answer your question about "biggest vulnerability", I think it's pertinent for you to understand our processes before we answer this. We have a team at Tridium dedicated to testing for security vulnerabilities, and in doing so, we also make sure that any third-party software and protocols that we use also don't have vulnerabilities. Vulnerabilities in open protocols (ex: SSL/TLS/WPA) and third-party software (including Java) are constantly being reported (ex: Java vulnerabilities are now reported quarterly), and it's important that we continue to patch and fix any that are reported to protect our customers.

   There are a number of publicly-known vulnerabilities related to protocols (SSL/TLS/Secure Wifi) that have been announced over the years, as well as vulnerabilities where we worked with external security researchers and organizations like US-CERT and ICS-CERT to fix, release a patch or new version of Niagara, and then work to publicly disclose the vulnerability. As we continue to test our product for security vulnerabilities, we are constantly rolling in fixes and security enhancements of our products, so the most up-to-date version of our products are always the most secure.

   If you have an older version of Niagara that is not up-to-date, there are a large number of vulnerabilities – and many of these are publicly known. AX is about to go end-of-life. Please upgrade to the latest version of Niagara and use the JACE-8000, in by doing this, you will get the benefit of the fixes, enhancements, and new security controls by our dedicated security team.

7. Has it been determined if JACEs are impacted by Ripple20 vulnerabilities? Have Tridium or hardware partners released a statement??

   https://www.tridium.com/~/media/tridium/library/documents/collateral/technicalbulletins/sb2020-tridium-3.ashx?la=en

8. Is there a way to subscribe to the latest Tridium cybersecurity information or mandatory patches?

   To receive Tridium communications, please subscribe via https://pages1.tridium.com/2018-GDPR---Website-Form_Sign-Up-page.html. This Subscribe link can also be found in the footer of www.Tridium.com.

9. Why doesn't the Niagara SLA include anything from a Honeywell partnered/owned Certificate Authority for the duration of the SLA for web access? OT integrators are left with self-signing to get/keep things running short of secondary IT knowledge and investment - which just doesn't exist or happen in many cases.

   Being a CA ourselves would be legally risky. A CA typically must perform business "background" checks to confirm ownership of domains, the business is in good standing, etc.

10. What security is provided for MQTT messaging?

    Connections between the client and broker should utilize TLS encryption and require some authentication which might be certificate or username and password based.

11. Do JACEs support syslog forwarding to a remote log server such as Splunk?

    Currently the JACE does not support syslog forwarding.

12. What versions have been approved by the Govt for federal / DOD sites?

    The RMF (Risk Management Framework) guidelines for DOD state "Niagara 4 (or higher) and JACE 8000 (or higher). We did this to account for all the "dot revs" along the way (i.e. 4.1, 4.2, …etc..) There is also now RMF approval for the Edge 10 (which is simply written up as "Tridium Edge 10 device".)

13. What criteria do you use to make an immediate security fix versus waiting for the next release?

    High and critical issues are fixed as soon as they can and are typically backported to supported releases. Occasionally there are changes that cannot be backported and are incorporated into the next release. A security tech bulletin is normally published with these types of fixes. For medium and low issues, they are reviewed and if a patch can be generated, then that is generally done otherwise they are incorporated into the next release.

14. Do Niagara portability partners need to meet the same level of "secure by default" in their ports? Secure boot, hsm, etc?

    In our NPSDK documentation, we provide recommendations regarding security features/controls. During review, issues identified are assessed by the NPSDK team and recommendations for mitigation are returned to the portability partner.

15. Is there any manual for certificate procedure?

    doStationSecurity and other documents in the Niagara help system provide details.

16. Does 4.8 not support the SAML for third party feature?

    Niagara 4.4 and newer supports SAML 2.0 with third party IdP. Niagara 4.9 includes a native Niagara IdP service instead of requiring external IdP.

17. Is there any roadmap to have Whitelisting/Blacklisting of IPs/IP Ranges in Niagara? Web/FOXS/Others?

    There currently isn't a plan to do this for fox. In Niagara 4.8+, there is a whitelisting feature for the browser client (jxbrowser) in Workbench to prevent users from "browsing" to non-whitelisted addresses.

18. Is/will Tridium researching and advising OS and other patches and their compatibility with N4? A recommended approved patch list?

    We publish a list of approved OS platforms for supervisors, but we do not monitor for OS patches, etc. When patches are made available we make every effort to test them for any impact on Niagara. For JACEs, we work closely with QNX to identify issues and get mitigations where appropriate.

19. What are the recommended ways to scan for edge devices through a Jace from a building network? OWASP top 10.

    Many customers/partners use tools like Qualys, etc. for scanning hardware on their networks. Internally, every Niagara release gets tested with tools like Burpsuite, Qualys, etc. to help try and identify any new issues.

20. Is there a way to remove the "remember credentials" feature from the login box in Niagara?

    In the Workbench menu click Tools then Options and on the general tab there is "Allow User Credential Caching" which can be set to false. The result is the "Remember these credentials" option is disabled in the login dialog but still displayed.