ICS-CERT ALERT

ICS-ALERT-12-195-01—TRIDIUM NIAGARA DIRECTORY TRAVERSAL AND WEAK CREDENTIAL STORAGE VULNERABILITY

July 13, 2012

ALERT

SUMMARY

Independent security researchers Billy Rios and Terry McCorkle notified ICS-CERT of a directory traversal and weak credential storage vulnerability with proof-of-concept (PoC) exploit code for Tridium Niagara AX Framework[a] software. According to their research, the vulnerabilities are exploitable by downloading and decrypting the file containing the user credentials from the server.

ICS-CERT has been in coordination with Mr. Rios, Mr. McCorkle and Tridium. Original attempts to coordinate vulnerability information were unsuccessful and ICS-CERT, in coordination with the researchers, was planning a release of the vulnerability information. However, recent communications from Tridium indicated they were working on a solution, resulting in the delayed release of this Alert so that mitigations/patches could be prepared. Yesterday, a public report[b] was published detailing the vulnerabilities and as a result, ICS-CERT has shortened its release schedule and is issuing this Alert to warn the community of the unpatched vulnerabilities.

Tridium has released a security alert[c] with instructions on how to implement interim mitigations. Tridium has stated that they are testing a software update that will resolve these vulnerabilities.

ICS-CERT will issue an Advisory when the software update is available.

a. Tridium Products, http://www.tridium.com/cs/products_/_services/frameworks, Web site last accessed June 25, 2012.

b. Robert O'Harrow, "Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks," http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story html, Web site last accessed July 12, 2012.

c. Tridium Security Alert, https://www.tridium.com/galleries/briefings/NiagaraAX_Framework_Software_Security_Alert.pdf, Web site last accessed July 13, 2012.

Mr. Rios[d] and Mr. McCorkle's research includes vulnerability details for the following vulnerabilities:

Vulnerability Type	Remotely Exploitable	Impact
Directory traversal	Yes	Data leakage
Weak credential storage	Yes	Privilege escalation

BACKGROUND

Tridium Niagara is a software platform that integrates various different systems and devices and allows them to be managed via the Internet.

Tridium sells its products and services through multiple distribution channels, which include OEMs/resellers, independent systems integrators, and energy service companies. According to the Tridium Web site, over 300,000 instances of Niagara AX Framework are installed worldwide in applications that include energy management, building automation, telecommunications, security automation, machine to machine (M2M), lighting control, maintenance repair operations (MRO), service bureaus and total facilities management.[e]

MITIGATION

Tridium recommends the following mitigations.

- Disable the "guest" and "demo" user accounts if enabled.
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts.
- Use strong passwords.
- Change default credentials
- Limit user access to the file system following the instructions in the Niagara AX Framework Software Security Alert below
- Ensure that control systems are not directly Internet facing.

Tridium has released a Niagara AX Framework Software Security Alert available here: https://www.tridium.com/galleries/briefings/NiagaraAX_Framework_Software_Security_Alert.pdf

Because each control system installation is unique, owners and operators may need to contact their system vendor or integrator for assistance.

d. Billy Rios Blog, http://xs-sniper.com/blog/ Web site last accessed July 13, 2012
e. Tridium Niagara, http://www.tridium.com/cs/corporate_info/faqs, Web site last accessed June 25, 2012.

Owners and operators can also perform a comprehensive control system cybersecurity assessment using the DHS Control Systems Security Program (CSSP) Cyber Security Evaluation Tool (CSET)[f]. CSET is a free, downloadable, stand alone software tool that is designed to assist owners and operators to:

- determine their current security posture,
- identify where security improvements can/should be made,
- map out the existing component/network configuration, and
- output a basic cybersecurity plan.

A CSET fact sheet is available on the CSSP Web page; it explains the self-evaluation process and provides further information and assistance with the tool. The tool can be downloaded online or organizations can contact CSSP to request onsite training and guidance.

In addition, ICS-CERT recommends that control system owners and operators take defensive measures to minimize the risk of exploitation of these vulnerabilities. ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[g]

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

f. CSET, http://www.us-cert.gov/control_systems/satool.html, Web site last accessed July 13, 2012.

g. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, Web site last accessed June 25, 2012.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
Email: ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.