ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-228-01—TRIDIUM NIAGARA MULTIPLE VULNERABILITIES

August 15 2012

OVERVIEW

This advisory is a follow-up to "ICS-ALERT-12-195-01—Tridium Niagara Directory Traversal and Weak Credential Storage Vulnerability" that was published July 13, 2012, on the ICS-CERT Web page.

Independent security researchers Billy Rios and Terry McCorkle have identified multiple vulnerabilities in the Tridium Niagara AX Framework software. The vulnerabilities include directory traversal, weak credential storage, session cookie weaknesses, and predictable session IDs, all of which can be exploited remotely. Although not all technical details have been released, these vulnerabilities have been made public.

Tridium has issued a security alert[a], and has produced a patch that Mr. Rios and Mr. McCorkle have validated fixes these vulnerabilities.

AFFECTED PRODUCTS

All known versions of the Tridium Niagara AX Framework software products are susceptible to these vulnerabilities.

IMPACT

Successfully exploiting these vulnerabilities will lead to data leakage and possible privilege escalation.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

The Tridium Niagara AX software platform integrates different systems and devices, e.g., HVAC, building automation controls, telecommunications, security automation, machine–to-

[a] Tridium Announcements, http://www.tridium.com/cs/tridium_news/security_patch_36, Web site last accessed August 14, 2012.

machine (M2M), lighting control, maintenance repair operations (MRO), service bureaus, and facilities management[b], onto a single platform that can be managed and controlled over the Internet from a Web browser.

Tridium sells its products and services through multiple distribution channels, which include OEMs/resellers, independent systems integrators, and energy service companies. According to Tridium, more than 300,000 instances of Niagara AX Framework are installed worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DIRECTORY TRAVERSAL[c]

By default, the Tridium Niagara AX software is not configured to deny access to restricted parent directories. This vulnerability allows a successful attacker to access the file that stores all system usernames and passwords. An attacker could exploit this vulnerability by sending a specially crafted request to the Web server running on Port 80/TCP.

CVE-2012-4027[d] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is ((AV:N/AC:M/Au:S/C:C/I:N/A:N).[e]

WEAK CREDENTIAL STORAGE[f]

The system insecurely stores user authentication credentials, which are susceptible to interception and retrieval. User authentication credentials are stored in the Niagara station configuration file, config.bog, which is located in the root of the station folder.

CVE-2012-4028[g] has been assigned to this vulnerability. A CVSS v2 base score of 6.5 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:S/C:C/I:C/A:C).[h]

[b] Tridium Niagara, http://www.tridium.com/cs/corporate_info/faqs, Web site last accessed August 14, 2012.

[c] CWE, http://cwe.mitre.org/data/definitions/22.html, Web site last accessed August 14, 2012.

[d] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4027 , Web site last accessed August 14, 2012.

[e] NVD, http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2, Web site last accessed August 14, 2012.

[f] CWE, http://cwe.mitre.org/data/definitions/522, Web site last accessed August 14, 2012.

[g] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4028, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[h] NVD, http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2, Web site last accessed August 14, 2012.

PLAINTEXT STORAGE IN A COOKIE[i]

Usernames and passwords are stored using Base64 encoding in a cookie within the default authentication configuration. This significantly lowers the difficulty of exploitation by an attacker. The user must take additional steps to configure stronger authentication.

CVE-2012-3025[j] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:C/A:N)

PREDICTABLE SESSION IDS[k]

The software generates a predictable session ID or key value, allowing an attacker to guess the session ID or key.

CVE-2012-3024[l] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:C/A:N)

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities can be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target some of these vulnerabilities are publicly available, although not all technical details have been released.

DIFFICULTY

An attacker with a medium skill could exploit these vulnerabilities.

MITIGATION

To mitigate the decoding of passwords listed in the config.bog file, Tridium recommends that security settings for file access be assigned only at the administrator level. Instructions for

[i] CWE, http://cwe.mitre.org/data/definitions/315.html, Web site last accessed August 14, 2012.

[j] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3025, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[k] CWE, http://cwe.mitre.org/data/definitions/330.html, Web site last accessed August 14, 2012.

[l] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3024, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

configuring these settings are included in the July 13 Security Alert[m] from Tridium. In addition, Tridium has issued a patch that prevents access to the config.bog file and backups of the file from network facing clients. The patch can be found at this URL:

https://www.niagara-central.com/ord?portal:/dev/wiki/Niagara_AX_3.5_and_3.6_Security_Patches

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Install 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), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[n] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01—Cyber Intrusion Mitigation Strategies,[o] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

[m] Tridium Announcements, http://www.tridium.com/cs/tridium_news/security_patch_36, Web site last accessed August 14, 2012.

[n] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 14, 2012.

[o] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed August 14, 2012.

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events 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.