



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-045-01—TRIDIUM NIAGARAAX DIRECTORY TRAVERSAL VULNERABILITY

February 14, 2013

OVERVIEW

This advisory provides mitigation details for a vulnerability in the Tridium NiagaraAX software. Independent researchers Billy Rios and Terry McCorkle discovered a directory traversal vulnerability in the Tridium NiagaraAX software product. They demonstrated that with a valid user account or guest privileges enabled, privilege escalation is possible on a NiagaraAX system. Exploitation of this vulnerability could allow loss of availability, integrity, and confidentiality of the system.

Tridium has produced a patch that mitigates this vulnerability. This vulnerability is remotely exploitable.

AFFECTED PRODUCTS

The following Tridium products are affected:

- Tridium NiagaraAX,^a all versions.

IMPACT

A loss of integrity, data, and possibly physical damage can result if the software is being used to control a physical process. Another consequence might be the compromise of facility security where NiagaraAX is used for facility access control and administration.

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

a. Tridium NiagaraAX - http://www.tridium.com/cs/products/_services/niagaraax, last visited February 14, 2013.

This product is provided subject only to the Notification Section as indicated here: <http://www.us-cert.gov/privacy/>



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

BACKGROUND

Tridium is a US-based company that maintains offices in several countries around the world, including the US, UK, Singapore, and China. Tridium also deploys systems to Latin America.

NiagaraAX is a general framework that can be used to integrate and manage diverse industrial control system components, e.g., HVAC, building automation controls, and facility management that can be controlled over the Internet from a Web browser. According to Tridium, more than 350,000 instances of the NiagaraAX Framework are used worldwide.

Tridium estimates that these products are used primarily in the commercial facilities (88 percent), energy (5 percent), education (5 percent), and government facilities and other sectors (2 percent).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

PATH TRAVERSAL^b

If an installed NiagaraAX instance has its Web interface accessible from the Internet, and the user has valid user credentials, or if the system's guest user function is enabled, the application could be subverted to escalate the user's credentials and gain control of the system. The attacker could read the contents of unexpected files, expose sensitive data, execute arbitrary code, and affect the availability by sending a specially crafted packet to the Web server on Port 80/TCP.

CVE-2012-4701^c has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/C:C/I:C/A:C).^d If the guest user function is enabled, no authentication is required to exploit this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely.

b. CWE-22, <http://cwe.mitre.org/data/definitions/22.html>, CWE-22: Path Traversal, Web site last accessed February 14, 2013.

c. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4701>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:M/Au:S/C:C/I:C/A:C\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:C/I:C/A:C)), Web site last visited February 14, 2013.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with medium skill may be able to exploit this vulnerability.

MITIGATION

Tridium has developed patches for all current versions (Versions 3.5, 3.6, and 3.7) of the NiagaraAX software. Links to the patches, along with instructions on their use, can be obtained from the Tridium Security Update Web page: https://www.niagara-central.com/ord?portal:/dev/wiki/Niagara_AX_Security_Patch_11-Feb-2013.

For users of older versions of NiagaraAX software (prior to Version 3.5), Tridium recommends that users either upgrade to the newest version or take careful measures to isolate access to the Web interface from the Internet. Users are encouraged to contact Tridium for details on disabling the Web interface and for information on how to get to the most current version of NiagaraAX.

- 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.
- 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), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.^e 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-12-146-01B—Targeted Cyber Intrusion

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed February 14, 2013.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Detection and Mitigation Strategies,^f 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:

Email: ics-cert@hq.dhs.gov

Toll Free: 1-877-776-7585

For industrial control systems security 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.

f. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed February 14, 2013.