SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Cyber Alert
Newark Division

23 July 2012

SIR Number: SIR-00000003417

(U//FOUO) Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Access to a New Jersey Company's Industrial Control System

SOURCE: (U//FOUO) An FBI agent.

(U//FOUO) In February and March 2012, unauthorized IP addresses accessed the Industrial Control System (ICS) network of a New Jersey air conditioning company, US Business 1. The intruders were able to access a backdoor into the ICS system that allowed access to the main control mechanism for the company's internal heating, ventilation, and air conditioning (HVAC) units. US Business 1 was using the Tridium Niagara ICS system, which has been widely reported in the media to contain multiple vulnerabilities that could allow an attacker to remotely control the system.

(U//FOUO) On 21 and 23 January 2012, an unknown subject posted comments on a known US website, titled "#US #SCADA #IDIOTS" and "#US #SCADA #IDIOTS part-II". The postings were linked to the moniker "@ntisec", and indicated that hackers were targeting SCADA systems this year, and something had to be done to address SCADA vulnerabilities. [1]

1. (U) Anti-sec (or the Anti Security Movement) is a movement opposed to the full disclosure of software vulnerabilities and exploits, a process that it believes is is used by the computer security sector to market computer security products.

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the Newark Division and has not been vetted by FBI Headquarters.

(U) The user of the "@ntisec" moniker searched Google, and the website www.shodanhq.com, for the term ":(unknown character) slot:/" and "#TRIDIUM / #NIAGARA vector". The posting by "@ntisec" included a list of URLs, one of which was an IP address that resolved to US Business 1, and was assigned to its office building's HVAC control system.

(U//FOUO) The main control box for the HVAC system of US Business 1 was a Tridium brand, Niagara model controller. US Business 1 actively used this system in-house, but also installed the control system for customers, which included banking institutions and other commercial entities. An IT contractor of US Business 1 confirmed the Niagara control box was directly connected to the Internet with no interposing firewall.

(U//FOUO) US Business 1 had a controller for the system that was password protected, but was set up for remote/Internet access. By using the link posted by the hacktivist, the published backdoor URL provided the same level of access to the company's control system as the password-protected administrator login. The backdoor required no password and allowed direct access to the control system.

(U//FOUO) Logs from the controller at US Business 1 dated back to 3 February 2012, and access to the controller was found from multiple unauthorized international and US-based IP addresses. [2]

(U//FOUO) The URL that linked to the control system of US Business 1 provided access to a Graphical User Interface (GUI), which provided a floor plan layout of the office, with control fields and feedback for each office and shop area. All areas of the office were clearly labeled with employee names or area names.

(U) On 13 July 2012, the Department of Homeland Security released ICS-CERT ALERT entitled, "Tridium Niagara Directory Traversal and Weak Credential Storage Vulnerability", which detailed vulnerabilities within the Niagara AX ICS that are exploitable by downloading and decrypting the file containing the user credential from the server.

(U) According to the Tridium website, over 300,000 instances of Niagara AX Framework are installed worldwide in applications that include energy management, building automation, telecommunications, security automation and lighting control. [3]

(U) This report has been prepared by the Newark Division of the FBI. Comments and queries may be addressed to the Newark Field Intelligence Group at 973-792-3000.

2. (U) For more information regarding the international IP addresses that accessed the network of US Business 1, cite FBI IIR 4 213 3107 12; DTG R 201441Z APR 12; classified title; from a contact with excellent access who spoke in confidence.
3. (U) Tridium Niagara, http://www.tridium.com/cs/corporate_info/faqs, website last accessed July 18, 2012.

Distribution

Deputy Assistant Director, Directorate of Intelligence
FBI Intranet
National Security Analysis and Production Branch
New Jersey Regional Operations and Intelligence Center
New Jersey State Police
Production Services Unit, Directorate of Intelligence

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:

Federal Bureau of Investigation
Newark
11 Centre Place
Newark, NJ 07102
Fax: (973) 792-3035

Customer and Product Information

SIR Tracking ID: SIR-00000003417
Product Title: Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Access to a New Jersey Company's Industrial Control System
Dated: _____
Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Actionable Value

2. The product helped me decide on a course of action. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Timeliness Value

3. The product was timely to my needs. (Check one)
   ___5. Strongly Agree
   ___4. Somewhat Agree
   ___3. Neither Agree or Disagree
   ___2. Somewhat Disagree
   ___1. Strongly Disagree

Comments (please use reverse or attach separate page if needed):
_____
_____
_____
_____