More ICS-CERT Advisories

ICS Advisory (ICSA-15-090-01)

Inductive Automation Ignition Vulnerabilities

Original release date: March 31, 2015 | Last revised: August 27, 2018

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

OVERVIEW

Evgeny Druzhinin, Alexey Osipov, Ilya Karpov, and Gleb Gritsai of Positive Technologies have identified several vulnerabilities in Inductive Automation’s Ignition Software. Inductive Automation has produced a patch that mitigates these vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Inductive Automation product is affected:

- Inductive Automation Ignition 7.7.2

IMPACT

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

BACKGROUND

Inductive Automation is a Folsom, California-based supplier of web-based industrial automation software.

The affected product, Ignition, is an updated version of FactoryPMI, offered by Inductive Automation. Ignition is a human-machine interface/SCADA product used in a variety of industrial applications. According to Inductive Automation, Ignition is deployed across several sectors including Communications, Energy, Food and Agriculture, and Water and Wastewater Systems. Inductive Automation estimates that this product is used primarily in North and South America, Europe, Australia, and across Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTING (XSS)a

An attacker may cause dangerous content to be executed through a vulnerable web application. The server reads data directly from the HTTP request and reflects it back in the HTTP response.

CVE-2015-0976b has been assigned to this vulnerability. A CVSS v2 base score of 5.9 has been assigned; the CVSS vector string is (AV:L/AC:H/Au:N/C:C/I:C/A:P).c

INFORMATION EXPOSURE THROUGH ERROR MESSAGEd

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

CVE-2015-0991e 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:L/Au:N/C:P/I:N/A:N).f

INSECURE STORAGE OF SENSITIVE INFORMATIONg

OPC Server username and password stored in setting file is in clear text.

CVE-2015-0992h has been assigned to this vulnerability. A CVSS v2 base score of 5.2 has been assigned; the CVSS vector string is (AV:L/AC:L/Au:S/C:C/I:P/A:N).i

INSUFFICIENT SESSION EXPIRATIONj

After user logs out, the session is not removed. This could lead to session reuse by attacker with privileges of the same user.

CVE-2015-0993k has been assigned to this vulnerability. A CVSS v2 base score of 5.5 has been assigned; the CVSS vector string is (AV:A/AC:H/Au:S/C:P/I:C/A:P).l

CREDENTIALS MANAGEMENTm

The mechanism of blocking brute force attacks could be bypassed with resetting session id parameter in HTTP request.

CVE-2015-0994n has been assigned to this vulnerability. A CVSS v2 base score of 4.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:S/C:P/I:P/A:P).o

USE OF PASSWORD HASH WITH INSUFFICIENT COMPUTATIONAL EFFORTp

Database storage of accounts by default in Windows and Database storage of accounts by default in Linux. Used hash algorithm - MD5, is known to be vulnerable to brute force attacks and not considered secure.

CVE-2015-0995q has been assigned to this vulnerability. A CVSS v2 base score of 9.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:C/I:C/A:C).r

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed URL to the JNLP.

EXISTENCE OF EXPLOIT

Exploits that target these vulnerabilities are not publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

Inductive Automation has developed a patch for these vulnerabilities and recommends updating as soon as possible. The patch is available at:

https://www.inductiveautomation.com/downloads/ignition

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

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

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

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.

- aCWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), http://cwe.mitre.org/data/definitions/79.html, web site last accessed March 31, 2015.
- bNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0976, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- cCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:L/AC:H/Au:N/C:C/I:C/A:P, web site last accessed March 31, 2015.
- dCWE-209: Information Exposure Through an Error Message http://cwe.mitre.org/data/definitions/209.html, web site last accessed March 31, 2015.
- eNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0991, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- fCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N, web site last accessed March 31, 2015.
- gCWE-922: Insecure Storage of Sensitive Information http://cwe.mitre.org/data/definitions/922.html, web site last accessed March 31, 2015.
- hNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0992, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- iCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:L/AC:L/Au:S/C:C/I:P/A:N, web site last accessed March 31, 2015.

- jCWE-613: Insufficient Session Expiration , https://cwe.mitre.org/data/definitions/613.html, web site last accessed March 31, 2015.
- kNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0993, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- lCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:A/AC:H/Au:S/C:P/I:C/A:P, web site last accessed March 31, 2015.
- mCWE-255: Credentials Management https://cwe.mitre.org/data/definitions/255.html, web site last accessed March 31, 2015.
- nNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0994, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- oCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:H/Au:S/C:P/I:P/A:P, web site last accessed March 31, 2015.
- pCWE-916: Use of Password Hash With Insufficient Computational Effort http://cwe.mitre.org/data/definitions/916.html, web site last accessed March 31, 2015.
- qNVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0995, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
- rCVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:S/C:C/I:C/A:C, web site last accessed March 31, 2015.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.