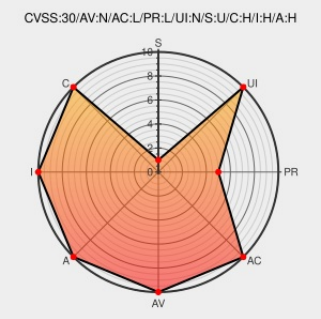
CVE-2022-35870

Published on: Not Yet Published

Last Modified on: 08/03/2022 04:53:00 PM UTC

CVE-2022-35870

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ignition from Inductiveautomation contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within com.inductiveautomation.metro.impl. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-17265.

CVE-2022-35870 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Inductive Automation** - **Ignition** version **8.1.15 (b2022030114)**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Security check	support.inductiveautomation.com text/html Inactive Link Not Archived	MISC support.inductiveautomation.com/hc/en-us/articles/7625759776653-Regarding-Pwn2Own-2022-Vulnerabilities
ZDI-22-1017 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-22-1017/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inductiveautomation	Ignition	8.1.15	All	All	All

cpe:2.3:a:inductiveautomation:ignition:8.1.15:*:*:*:*:*:*:*:

Discovery Credit

@_s_n_t of @pentestltd

Social Mentions

Source	Title	Posted (UTC)
@TheZDIBugs	[ZDI-22-1017|CVE-2022-35870] (Pwn2Own) Inductive Automation Ignition Deserialization of Untrusted Data Remote Code… twitter.com/i/web/status/1…	2022-07-15 19:48:24
@CVEreport	CVE-2022-35870 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of… twitter.com/i/web/status/1…	2022-07-25 18:25:28
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-35870 This vulnerability allows remote attackers to execute arbitrary c… twitter.com/i/web/status/1…	2022-07-25 20:56:01
@LinInfoSec	Metro - CVE-2022-35870: zerodayinitiative.com/advisories/ZDI…	2022-07-25 22:01:03
/r/netcve	CVE-2022-35870	2022-07-25 19:38:28

← Previous ID Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report