



# CVE-2022-21941

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-21941
<b>State</b>	PUBLIC
<b>Assigner</b>	productsecurity@jci.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-31 16:15:00 UTC
<b>Updated</b>	2022-10-01 02:30:00 UTC
<b>Description</b>	All versions of iSTAR Ultra prior to version 6.8.9.CU01 are vulnerable to a command injection that could allow an unauthenticated user to execute arbitrary commands on the affected device.

## Risk And Classification

**Problem Types:** CWE-77

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Johnsoncontrols</a>	Istar Ultra	-	All	All	All
Operating System	<a href="#">Johnsoncontrols</a>	Istar Ultra Firmware	All	All	All	All

## References

Reference	Source	Link	Tags
Product Security Advisories	CONFIRM	<a href="http://www.johnsoncontrols.com">www.johnsoncontrols.com</a>	
Sensormatic Electronics iSTAR   CISA	CERT	<a href="http://www.cisa.gov">www.cisa.gov</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Khoa Hoang

There are currently no legacy QID mappings associated with this CVE.

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 registered 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](#)**