



# CVE-2022-3752

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

## Summary

<b>CVE</b>	CVE-2022-3752
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT@rockwellautomation.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-19 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:51:00 UTC
<b>Description</b>	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Rockwellautomation</a>	Compactlogix 5380	-	All	All	All
Operating System	<a href="#">Rockwellautomation</a>	Compactlogix 5380 Firmware	All	All	All	All
Hardware	<a href="#">Rockwellautomation</a>	Compactlogix 5480	-	All	All	All
Operating System	<a href="#">Rockwellautomation</a>	Compactlogix 5480 Firmware	All	All	All	All
Hardware	<a href="#">Rockwellautomation</a>	Compactlogix 5580	-	All	All	All
Operating System	<a href="#">Rockwellautomation</a>	Compactlogix 5580 Firmware	All	All	All	All
Hardware	<a href="#">Rockwellautomation</a>	Compact Guardlogix 5380	-	All	All	All
Operating System	<a href="#">Rockwellautomation</a>	Compact Guardlogix 5380 Firmware	All	All	All	All
Hardware	<a href="#">Rockwellautomation</a>	Guardlogix 5580	-	All	All	All
Operating System	<a href="#">Rockwellautomation</a>	Guardlogix 5580 Firmware	All	All	All	All

## References

Reference	Source	Link	Tags
Logix Controllers Vulnerable to Denial-of-Service Attack	MISC	<a href="https://rockwellautomation.custhelp.com">rockwellautomation.custhelp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

591250 Rockwell Automation Logix controllers Improper Input Validation Vulnerability (ICSA-22-342-03)

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)