CVE-2020-7559

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-7559
State	PUBLIC
Assigner	cybersecurity@schneider-electric.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-19 22:15:00 UTC
Updated	2022-02-03 13:48:00 UTC
Description	A CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists in PLC Simulator on

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Ecostruxure Control Expert	All	All	All	All
Application	Se	Ecostruxure Control Expert	All	All	All	All
Application	Se	Ecostruxure Control Expert	All	All	All	All

References

Reference	Source	Link	Tags
TALOS-2020-1140 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	www.talosintelligence.com	
Security Notification - PLC Simulator on EcoStruxure™ Control Expert | Schneider Electric	MISC	www.se.com	Patch,
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590719 Schneider Electric PLC Simulator on EcoStruxure Control Expert and Process Expert Multiple Vulnerabilities (SEVD-2020-315-07)