CVE-2019-10953

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-10953
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-17 15:29:00 UTC
Updated	2022-01-31 20:48:00 UTC
Description	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researcl

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Abb	Pm554-tp-eth	-	All	All	All
Hardware	Abb	Pm554-tp-eth	-	All	All	All
Operating System	Abb	Pm554-tp-eth Firmware	-	All	All	All
Operating System	Abb	Pm554-tp-eth Firmware	-	All	All	All
Hardware	Phoenixcontact	Ilc 151 Eth	-	All	All	All
Hardware	Phoenixcontact	Ilc 151 Eth	-	All	All	All
Operating System	Phoenixcontact	Ilc 151 Eth Firmware	-	All	All	All
Operating System	Phoenixcontact	Ilc 151 Eth Firmware	-	All	All	All
Hardware	Schneider-electric	Modicon M221	-	All	All	All
Hardware	Schneider-electric	Modicon M221	-	All	All	All
Operating System	Schneider-electric	Modicon M221 Firmware	All	All	All	All
Operating System	Schneider-electric	Modicon M221 Firmware	All	All	All	All
Hardware	Se	Modicon M221	-	All	All	All
Operating System	Se	Modicon M221 Firmware	All	All	All	All
Hardware	Siemens	6ed1052-1cc01-0ba8	-	All	All	All
Hardware	Siemens	6ed1052-1cc01-0ba8	-	All	All	All
Operating System	Siemens	6ed1052-1cc01-0ba8 Firmware	-	All	All	All

Operating System	Siemens	6ed1052-1cc01-0ba8 Firmware	-	All	All	All
Hardware	Siemens	6es7211-1ae40-0xb0	-	All	All	All
Hardware	Siemens	6es7211-1ae40-0xb0	-	All	All	All
Operating System	Siemens	6es7211-1ae40-0xb0 Firmware	-	All	All	All
Operating System	Siemens	6es7211-1ae40-0xb0 Firmware	-	All	All	All
Hardware	Siemens	6es7314-6eh04-0ab0	-	All	All	All
Hardware	Siemens	6es7314-6eh04-0ab0	-	All	All	All
Operating System	Siemens	6es7314-6eh04-0ab0 Firmware	-	All	All	All
Operating System	Siemens	6es7314-6eh04-0ab0 Firmware	-	All	All	All
Hardware	Wago	Bacnet/ip	-	All	All	All
Operating System	Wago	Bacnet/ip Firmware	-	All	All	All
Hardware	Wago	Bacnet/ip	-	All	All	All
Hardware	Wago	Bacnet/ip	-	All	All	All
Operating System	Wago	Bacnet/ip Firmware	-	All	All	All
Operating System	Wago	Bacnet/ip Firmware	-	All	All	All
Hardware	Wago	Ethernet	-	All	All	All
Hardware	Wago	Ethernet	-	All	All	All
Operating System	Wago	Ethernet Firmware	-	All	All	All
Operating System	Wago	Ethernet Firmware	-	All	All	All
Hardware	Wago	Knx Ip	-	All	All	All
Hardware	Wago	Knx Ip	-	All	All	All
Operating System	Wago	Knx Ip Firmware	-	All	All	All
Operating System	Wago	Knx Ip Firmware	-	All	All	All
Hardware	Wago	Pfc100	-	All	All	All
Hardware	Wago	Pfc100	-	All	All	All
Operating System	Wago	Pfc100 Firmware	-	All	All	All
Operating System	Wago	Pfc100 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Malformed Request	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
PLC Cycle Time Influences | ICS-CERT	MISC	ics-cert.us-cert.gov	Mitigation, Third Party Advisory, US Government Resource
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© 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 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