termination on the buffer sp+0x40 since it overflowed into sp+0x440. The strcpy() will result in invalid memory access. An state value of length 0x3c9 will cause the service to crash."> using sprintf(). The destination buffer sp+0x40 is overflowed with the call to sprintf() for any state values that are greater than 512-len("/etc/config-tools/config_interfaces interface=X1 state=") in length. Later, at 0x1ea08 strcpy() is used to copy the contents of the stack buffer that was overflowed sp+0x40 into sp+0x440. The buffer sp+0x440 is immediately adjacent to sp+0x40 on the stack. Therefore, there is no NULL termination on the buffer sp+0x40 since it overflowed into sp+0x440. The strcpy() will result in invalid memory access. An state value of length 0x3c9 will cause the service to crash." />

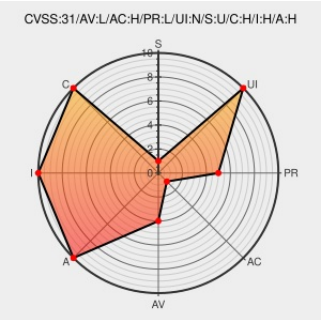
CVE-2019-5185

Published on: 03/23/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-5185

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



Certain versions of Pfc200 from Wago contain the following vulnerability:

An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200. An attacker can send a specially crafted packet to trigger the parsing of this cache file. At 0x1ea28 the extracted state value from the xml file is used as an argument to /etc/config-tools/config_interfaces interface=X1 state=<contents of state node> using sprintf(). The destination buffer sp+0x40 is overflowed with the call to sprintf() for any state values that are greater than 512-len("/etc/config-tools/config_interfaces interface=X1 state=") in length. Later, at 0x1ea08 strcpy() is used to copy the contents of the stack buffer that was overflowed sp+0x40 into sp+0x440. The buffer sp+0x440 is immediately adjacent to sp+0x40 on the stack. Therefore, there is no NULL termination on the buffer sp+0x40 since it overflowed into sp+0x440. The strcpy() will result in invalid memory access. An state value of length 0x3c9 will cause the service to crash.

CVE-2019-5185 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
TALOS-2019-0966 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0966

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
Hardware	Wago	Pfc200	-	All	All	All
Hardware	Wago	Pfc200	-	All	All	All
Operating System	Wago	Pfc200 Firmware	03.02.02(14)	All	All	All
Operating System	Wago	Pfc200 Firmware	03.02.02\(14\)	All	All	All
Operating System	Wago	Pfc200 Firmware	03.02.02\(14\)	All	All	All

cpe:2.3:h:wago:pfc200:-:*:*:*:*:*:*:*:

cpe:2.3:h:wago:pfc200:-:*:*:*:*:*:*:*:

cpe:2.3:o:wago:pfc200_firmware:03.02.02(14):*:*:*:*:*:*:*:

cpe:2.3:o:wago:pfc200_firmware:03.02.02\(14\):*:*:*:*:*:*:*:

cpe:2.3:o:wago:pfc200_firmware:03.02.02\(14\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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