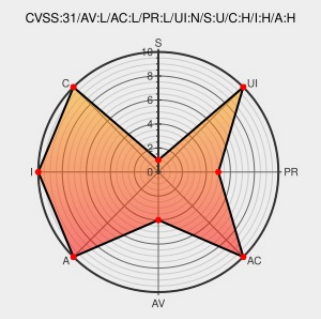
CVE-2019-5166

Published on: 03/10/2020 12:00:00 AM UTC

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

CVE-2019-5166

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



Certain versions of Pfc200 from Wago contain the following vulnerability:

An exploitable stack buffer overflow vulnerability exists in the iocheckd service 'I/O-Check' functionality of WAGO PFC 200 version 03.02.02(14). A specially crafted XML cache file written to a specific location on the device can cause a stack buffer overflow, resulting in code execution. An attacker can send a specially crafted packet to trigger the parsing of this cache file.

CVE-2019-5166 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Wago** - **WAGO PFC200 Firmware** version **version 03.02.02(14)**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link

TALOS-2019-0961 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Mitigation Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0961

Related QID Numbers

590952 WAGO PFC200 iocheckd service cache Domain Name System (DNS) Remote Code Execution (RCE) Vulnerability (TALOS-2019-0961)

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 and Source URL Uptime Status status.cve.report