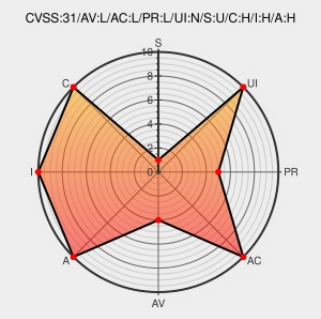
# CVE-2019-5181

Published on: 03/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

## CVE-2019-5181

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 Firmware 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. The destination buffer sp+0x440 is overflowed with the call to sprintf() for any subnetmask values that are greater than 1024-len('/etc/config-tools/config_interfaces interface=X1 state=enabled subnet-mask=') in length. A subnetmask value of length 0x3d9 will cause the service to crash.

CVE-2019-5181 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Wago** - **WAGO PFC200** version **Firmware 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-2019-0963 \|\| Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | Exploit<br>Technical Description<br>Third Party Advisory<br>talosintelligence.com<br>text/html | MISC<br>talosintelligence.com/vulnerability_reports/TALOS-2019-0963 |



## Related QID Numbers

591135 WAGO PFC200 iocheckd service "I/O-Check" cache Multiple Code Execution Multiple Vulnerabilities (TALOS-2019-0963)

## 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**