



# CVE-2019-5081

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-5081
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-18 20:15:00 UTC
<b>Updated</b>	2021-07-21 11:39:00 UTC
<b>Description</b>	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Chec" functionality of WAGO PFC 200 F

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Wago</a>	<a href="#">Pfc 100</a>	-	All	All	All
Hardware	<a href="#">Wago</a>	<a href="#">Pfc 100</a>	-	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 100 Firmware</a>	03.00.39(12)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 100 Firmware</a>	03.00.39(12\)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 100 Firmware</a>	03.00.39(12\)	All	All	All
Hardware	<a href="#">Wago</a>	<a href="#">Pfc 200</a>	-	All	All	All
Hardware	<a href="#">Wago</a>	<a href="#">Pfc 200</a>	-	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.00.39(12)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.00.39(12\)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.01.07(13)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.01.07(13\)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.00.39(12\)	All	All	All
Operating System	<a href="#">Wago</a>	<a href="#">Pfc 200 Firmware</a>	03.01.07(13\)	All	All	All

## References

Reference	Source	Link	Tags
TALOS-2019-0874    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="http://www.talosintelligence.com">www.talosintelligence.com</a>	Exploit,

TALOS-2019-0873    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	<a href="https://talosintelligence.com">talosintelligence.com</a>	Exploit,
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[590455](#) WAGO I/O-CHECK Multiple Vulnerabilities (ICSA-20-065-01)

© [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 registered 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](#)