



# CVE-2022-21194

Published on: Not Yet Published

Last Modified on: 03/18/2022 02:38:00 PM UTC

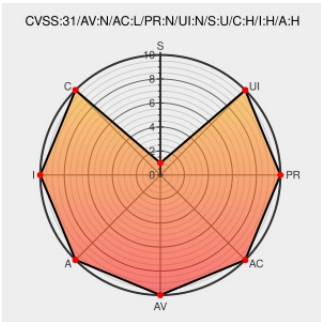
## CVE-2022-21194

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Centum Vp** from **Yokogawa** contain the following vulnerability:

The following Yokogawa Electric products do not change the passwords of the internal Windows accounts from the initial configuration: CENTUM VP versions from R5.01.00 to R5.04.20 and versions from R6.01.00 to R6.08.0, Exaopc versions from R3.72.00 to R3.79.00.

CVE-2022-21194 has been assigned by [vultures@jpcert.or.jp](mailto:vultures@jpcert.or.jp) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Yokogawa Electric Corporation](#) - **CENTUM VP** version **versions from R5.01.00 to R5.04.20**

Affected Vendor/Software: [Yokogawa Electric Corporation](#) - **CENTUM VP** version **versions from R6.01.00 to R6.08.00**

Affected Vendor/Software: [Yokogawa Electric Corporation](#) - **Exaopc** version **versions from R3.72.00 to R3.79.00**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
	<a href="#">web-material3.yokogawa.com</a> <a href="#">application/pdf</a>	<a href="#">CONFIRM web-material3.yokogawa.com/1/32094/files/YSAR-22-0001-E.pdf</a>

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](mailto:comment@cve.report).

## Related QID Numbers

[590868](#) Yokogawa CENTUM Multiple Vulnerabilities (ICSA-22-083-01) (YSAR-22-0001)

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Yokogawa</a>	<a href="#">Centum Vp</a>	-	All	All	All
Hardware	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Entry</a>	-	All	All	All
Operating System	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Entry Firmware</a>	All	All	All	All
Operating System	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Entry Firmware</a>	All	All	All	All
Operating System	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Entry Firmware</a>	All	All	All	All
Operating System	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Firmware</a>	All	All	All	All
Operating System	<a href="#">Yokogawa</a>	<a href="#">Centum Vp Firmware</a>	All	All	All	All
Application	<a href="#">Yokogawa</a>	<a href="#">Exaopc</a>	All	All	All	All

cpe:2.3:h:yokogawa:centum\_vp:-:\*:\*:\*:\*:\*:

cpe:2.3:h:yokogawa:centum\_vp\_entry:-:\*:\*:\*:\*:\*:

cpe:2.3:o:yokogawa:centum\_vp\_entry\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:yokogawa:centum\_vp\_entry\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:yokogawa:centum\_vp\_entry\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:yokogawa:centum\_vp\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:yokogawa:centum\_vp\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:a:yokogawa:exaopc:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-21194 : The following Yokogawa Electric products do not change the passwords of the internal #Windows acco... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-03-11 09:17:14
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-21194 The following Yokogawa Electric products do not change the passwo... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-03-11 10:56:04
 /r/netcve	<a href="#">CVE-2022-21194</a>	2022-03-11 10:38:17

[← 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 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](#)