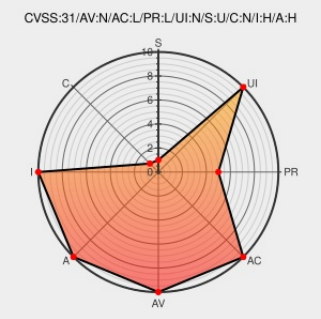
CVE-2022-21177

Published on: Not Yet Published

Last Modified on: 03/18/2022 02:09:00 PM UTC

CVE-2022-21177

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



Certain versions of Centum Cs 3000 from Yokogawa contain the following vulnerability:

There is a path traversal vulnerability in CAMS for HIS Log Server contained in the following Yokogawa Electric products: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, andfrom R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.

CVE-2022-21177 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Yokogawa Electric Corporation** - **CENTUM CS 3000** version **versions from R3.08.10 to R3.09.00**

Affected Vendor/Software: **Yokogawa Electric Corporation** - **CENTUM VP** version **versions from R4.01.00 to R4.03.00**

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: 8.1 - HIGH

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

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

Impact	Impact	Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	web-material3.yokogawa.com application/pdf	CONFIRM web-material3.yokogawa.com/1/32094/files/YSAR-22-0001-E.pdf

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.

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	Yokogawa	Centum Cs 3000	-	All	All	All
Hardware	Yokogawa	Centum Cs 3000 Entry	-	All	All	All
Operating System	Yokogawa	Centum Cs 3000 Entry Firmware	All	All	All	All
Operating System	Yokogawa	Centum Cs 3000 Firmware	All	All	All	All
Hardware	Yokogawa	Centum Vp	-	All	All	All
Hardware	Yokogawa	Centum Vp Entry	-	All	All	All
Operating System	Yokogawa	Centum Vp Entry Firmware	All	All	All	All
Operating System	Yokogawa	Centum Vp Entry Firmware	All	All	All	All
Operating System	Yokogawa	Centum Vp Entry Firmware	All	All	All	All
Operating System	Yokogawa	Centum Vp Firmware	All	All	All	All
Operating System	Yokogawa	Centum Vp Firmware	All	All	All	All
Operating System	Yokogawa	Centum Vp Firmware	All	All	All	All
Application	Yokogawa	Exaopc	All	All	All	All

cpe:2.3:h:yokogawa:centum_cs_3000:-:*:*:*:*:*:*:*:

cpe:2.3:h:yokogawa:centum_cs_3000_entry:-:*:*:*:*:*:*:*:

cpe:2.3:o:yokogawa:centum_cs_3000_entry_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:yokogawa:centum_cs_3000_firmware:*:*:*:*:*:*:*:*:

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: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-2022-21177 : There is a path traversal vulnerability in CAMS for HIS Log Server contained in the following Yoko… twitter.com/i/web/status/1…	2022-03-11 09:17:01
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-21177 There is a path traversal vulnerability in CAMS for HIS Log Serve… twitter.com/i/web/status/1…	2022-03-11 10:56:03
/r/netcve	CVE-2022-21177	2022-03-11 10:38:16

← Previous ID

Next ID→

© CVE.report 2022 |
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