



CVE-2014-5208

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

Summary

CVE	CVE-2014-5208
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-22 17:59:00 UTC
Updated	2014-12-22 19:27:00 UTC
Description	BKBCopyD.exe in the Batch Management Packages in Yokogawa CENTUM CS 3000 through R3.09.50 and CENTUM VP

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Yokogawa	Centum Cs 3000	-	All	All	All
Hardware	Yokogawa	Centum Cs 3000	-	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.01	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.02	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.03	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.04	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.05	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.06	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.07	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08.50	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08.70	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.09	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.09.50	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.01	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.02	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.03	All	All	All

Application	Yokogawa	Centum Cs 3000	r3.04	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.05	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.06	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.07	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08.50	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.08.70	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.09	All	All	All
Application	Yokogawa	Centum Cs 3000	r3.09.50	All	All	All
Hardware	Yokogawa	Centum Vp	-	All	All	All
Hardware	Yokogawa	Centum Vp	-	All	All	All
Application	Yokogawa	Centum Vp	r5.01.00	All	All	All
Application	Yokogawa	Centum Vp	r5.01.20	All	All	All
Application	Yokogawa	Centum Vp	r5.02.00	All	All	All
Application	Yokogawa	Centum Vp	r5.03.00	All	All	All
Application	Yokogawa	Centum Vp	r5.01.00	All	All	All
Application	Yokogawa	Centum Vp	r5.01.20	All	All	All
Application	Yokogawa	Centum Vp	r5.02.00	All	All	All
Application	Yokogawa	Centum Vp	r5.03.00	All	All	All
Application	Yokogawa	Centum Vp	All	All	All	All
Hardware	Yokogawa	Exaopc	-	All	All	All
Hardware	Yokogawa	Exaopc	-	All	All	All
Application	Yokogawa	Exaopc	All	All	All	All

References						
Reference			Source	Link	Tags	
R7-2014-10 Disclosure: Yokogawa CENTUM CS3000 B...			MISC	community.rapid7.com	Exploit	
Yokogawa CENTUM and Exaopc Vulnerability (Update A) ICS-CERT			MISC	ics-cert.us-cert.gov	Third Party Advisory,	
Sitemap Yokogawa Electric Corporation			CONFIRM	www.yokogawa.com	Vendor Advisory	
CVE Program record			CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail			NVD	nvd.nist.gov	canonical, analysis	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)