Yokogawa CENTUM CS 3000 Stack-based Buffer Overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0784
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-14 10:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Stack-based buffer overflow in BKBCopyD.exe in Yokogawa CENTUM CS 3000 R3.09.50 and earlier allows remote attacke

Risk And Classification

Primary CVSS: v2.0 8.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:C

Problem Types: CWE-121 | CWE-119 | CWE-121 CWE-121

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	8.3		AV:N/AC:M/Au:N/C:P/I:P/A:C
2.0	ics-cert@hq.dhs.gov	Secondary	8.3		AV:N/AC:M/Au:N/C:P/I:P/A:C
2.0	CNA	CVSS	8.3		AV:N/AC:M/Au:N/C:P/I:P/A:C

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Complete

AV:N/AC:M/Au:N/C:P/I:P/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yokogawa	CENTUM CS 3000	affected R3.09.50 custom	Not specified

References

Reference	Source	Link
Metasploit: R7-2013-19 Disclosure: Yokogawa CEN... | SecurityStreet	af854a3a-2127-422b-91ae-364da2661108	com
Yokogawa CENTUM CS 3000 Vulnerabilities (Update A) | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-c
www.cisa.gov/news-events/ics-advisories/icsa-14-070-01a	ics-cert@hq.dhs.gov	www
Yokogawa CENTUM CS3000 'BKBCopyD.exe' Stack Based Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www
www.securityfocus.com/bid/66130	ics-cert@hq.dhs.gov	www
www.yokogawa.com/dcs/security/ysar/dcs-ysar-index-en.htm.	ics-cert@hq.dhs.gov	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

CNA: Juan Vazquez of Rapid7 Inc. (en)

Additional Advisory Data

Solutions

CNA: Yokogawa has created a patch (CENTUM CS 3000 R3.09.73 and R3.09.75) to mitigate the reported vulnerabilities. To activate the patch software, the computer needs to be rebooted. Older versions of the CENTUM CS 3000 will need to be updated to the latest version of R3.09.50 before installing the patch software. Yokogawa also suggests all customers introduce appropriate security measures to the overall system, not just for the vulnerabilities identified. For more information, please see the advisory that Yokogawa has published regarding this issue here: http://www.yokogawa.com/dcs/security/ysar/dcs-ysar-index-en.htm .

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