



CVE-2010-4709

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

Summary

CVE	CVE-2010-4709
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-28 16:00:00 UTC
Updated	2017-08-17 01:33:00 UTC
Description	Heap-based buffer overflow in Automated Solutions Modbus/TCP Master OPC Server before 3.0.2 allows remote attackers

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.0	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.0a	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.0_build_1	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.1	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.10	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.11	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.12	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.12.1	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.12.3	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.2	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.2a	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.3	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.3a	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.4	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.4a	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.5	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.6	All	All	All

[illegible]

Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7a	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7b	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7c	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7d	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7e	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.7f	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.8	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.9	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.9.1	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.9.4	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.9.5	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	2.9_build_2.9.3	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	3.0.0	All	All	All
Application	Automatedsolutions	Modbus/tcp Master Opc Server	All	All	All	All

References	
Reference	Source
Automated Solutions Modbus/TCP OPC Server Remote Heap Corruption PoC	EXPLOIT-DB
404 - File Not Found CISA	MISC
ReadMe for Automated Solutions' Modbus/TCP OPC Server	CONFIRMED
Modbus/TCP Master OPC Server Packet Processing Buffer Overflow Vulnerability - Advisories - Community	SECURITY-FOCUS
IBM X-Force Exchange	XF
Automated Solutions Modbus/TCP OPC Server Remote Heap Corruption Vulnerability	BID
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULNERABILITY
US-CERT Vulnerability Note VU#768840 - Automated Solutions Modbus/TCP Master OPC server Modbus TCP header vulnerability	CERT
CVE Program record	CVE.CVE-2020-1000000
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report