OpenBMB XAgent API Key function_handler.py FunctionHandler.handle_tool_call log file

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4957
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 15:17:03 UTC
Updated	2026-03-30 13:26:29 UTC
Description	A flaw has been found in OpenBMB XAgent 1.0.0. The impacted element is the function FunctionHandler.handle_tool_call

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000350000 probability, percentile 0.102290000 (date 2026-04-02)

Problem Types: CWE-200 | CWE-532 | CWE-532 Sensitive Information in Log Files | CWE-200 Information Disclosure

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P/C..
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R
3.0	CNA	DECLARED	2.7	LOW	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	3.3		AV:N/AC:L/Au:M/C:P/I:N/A:N
2.0	CNA	DECLARED	3.3		AV:N/AC:L/Au:M/C:P/I:N/A:N/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenBMB	XAgent	affected 1.0.0	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	
vuldb.com	cna@vuldb.com	vuldb.com	
gist.github.com/YLChen-007/6279f3de0c2dff7732eaaf820843b562	cna@vuldb.com	gist.github.com	
vuldb.com	cna@vuldb.com	vuldb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Eric-z (VulDB User) (en)

CNA: VulDB (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-27T00:00:00.000Z	Advisory disclosed

CNA	2026-03-27T01:00:00.000Z	VulDB entry created
CNA	2026-03-27T09:13:11.000Z	VulDB entry last update

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