BigSweetPotatoStudio HyperChat AI Proxy Middleware aiProxyMiddleware.mts fetch server-side request forgery

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

Summary

CVE	CVE-2026-7223
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 04:16:29 UTC
Updated	2026-04-28 04:16:29 UTC
Description	A vulnerability was identified in BigSweetPotatoStudio HyperChat up to 2.0.0-alpha.63. Affected by this issue is the functior

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/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

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/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

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.0	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.1	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.2	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.3	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.4	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.5	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.6	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.7	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.8	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.9	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.10	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.11	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.12	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.13	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.14	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.15	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.16	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.17	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.18	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.19	Not specified

CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.20	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.21	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.22	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.23	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.24	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.25	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.26	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.27	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.28	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.29	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.30	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.31	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.32	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.33	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.34	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.35	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.36	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.37	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.38	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.39	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.40	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.41	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.42	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.43	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.44	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.45	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.46	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.47	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.48	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.49	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.50	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.51	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.52	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.53	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.54	Not specified

CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.55	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.56	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.57	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.58	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.59	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.60	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.61	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.62	Not specified
CNA	BigSweetPotatoStudio	HyperChat	affected 2.0.0-alpha.63	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/359823/cti	cna@vuldb.com	vuldb.com	
github.com/BigSweetPotatoStudio/HyperChat	cna@vuldb.com	github.com	
vuldb.com/vuln/359823	cna@vuldb.com	vuldb.com	
vuldb.com/submit/802265	cna@vuldb.com	vuldb.com	
github.com/BigSweetPotatoStudio/HyperChat/issues/142	cna@vuldb.com	github.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: BruceJin (VulDB User) (en)

CNA: VulDB CNA Team (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-27T00:00:00.000Z	Advisory disclosed
CNA	2026-04-27T02:00:00.000Z	VulDB entry created
CNA	2026-04-27T17:43:53.000Z	VulDB entry last update

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

Free CVE JSON API cve.report/api

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