CVE-2022-23064

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

Summary

CVE	CVE-2022-23064
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-02 13:15:00 UTC
Updated	2022-05-10 16:25:00 UTC
Description	In Snipe-IT, versions v3.0-alpha to v5.3.7 are vulnerable to Host Header Injection. By sending a specially crafted host head

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snipeitapp	Snipe-it	3.0.0	alpha1	All	All
Application	Snipeitapp	Snipe-it	3.0.0	alpha2	All	All
Application	Snipeitapp	Snipe-it	3.0.0	beta1	All	All
Application	Snipeitapp	Snipe-it	3.0.0	beta2	All	All
Application	Snipeitapp	Snipe-it	3.0.0	beta3	All	All
Application	Snipeitapp	Snipe-it	All	All	All	All

References

Reference	Source	Link
Force UrlGenerator's Root URL to be the base of APP_URL unless overriden · snipe/snipe-it@0c4768f · GitHub	MISC	github.com
CVE-2022-23064 | WhiteSource Vulnerability Database	MISC	www.whitesou
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: WhiteSource Vulnerability Research Team (WVR)

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