CVE-2014-4501

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

Summary

CVE	CVE-2014-4501
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-23 14:55:00 UTC
Updated	2014-07-23 18:07:00 UTC
Description	Multiple stack-based buffer overflows in sgminer before 4.2.2, cgminer before 4.3.5, and BFGMiner before 3.3.0 allow remo

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bfgminer	Bfgminer	3.2.0	All	All	All
Application	Bfgminer	Bfgminer	3.2.1	All	All	All
Application	Bfgminer	Bfgminer	3.2.2	All	All	All
Application	Bfgminer	Bfgminer	3.2.3	All	All	All
Application	Bfgminer	Bfgminer	3.2.4	All	All	All
Application	Bfgminer	Bfgminer	3.2.5	All	All	All
Application	Bfgminer	Bfgminer	3.2.6	All	All	All
Application	Bfgminer	Bfgminer	3.2.7	All	All	All
Application	Bfgminer	Bfgminer	3.2.8	All	All	All
Application	Bfgminer	Bfgminer	3.2.0	All	All	All
Application	Bfgminer	Bfgminer	3.2.1	All	All	All
Application	Bfgminer	Bfgminer	3.2.2	All	All	All
Application	Bfgminer	Bfgminer	3.2.3	All	All	All
Application	Bfgminer	Bfgminer	3.2.4	All	All	All
Application	Bfgminer	Bfgminer	3.2.5	All	All	All
Application	Bfgminer	Bfgminer	3.2.6	All	All	All
Application	Bfgminer	Bfgminer	3.2.7	All	All	All

Application	Bfgminer	Bfgminer	3.2.8	All	All	All
Application	Bfgminer	Bfgminer	All	All	All	All
Application	Cgminer Project	Cgminer	4.3.0	All	All	All
Application	Cgminer Project	Cgminer	4.3.1	All	All	All
Application	Cgminer Project	Cgminer	4.3.2	All	All	All
Application	Cgminer Project	Cgminer	4.3.3	All	All	All
Application	Cgminer Project	Cgminer	4.3.0	All	All	All
Application	Cgminer Project	Cgminer	4.3.1	All	All	All
Application	Cgminer Project	Cgminer	4.3.2	All	All	All
Application	Cgminer Project	Cgminer	4.3.3	All	All	All
Application	Cgminer Project	Cgminer	All	All	All	All
Application	Sgminer Project	Sgminer	4.0.0	All	All	All
Application	Sgminer Project	Sgminer	4.1.0	All	All	All
Application	Sgminer Project	Sgminer	4.1.153	All	All	All
Application	Sgminer Project	Sgminer	4.1.242	All	All	All
Application	Sgminer Project	Sgminer	4.1.271	All	All	All
Application	Sgminer Project	Sgminer	4.2.0	All	All	All
Application	Sgminer Project	Sgminer	4.0.0	All	All	All
Application	Sgminer Project	Sgminer	4.1.0	All	All	All
Application	Sgminer Project	Sgminer	4.1.153	All	All	All
Application	Sgminer Project	Sgminer	4.1.242	All	All	All
Application	Sgminer Project	Sgminer	4.1.271	All	All	All
Application	Sgminer Project	Sgminer	4.2.0	All	All	All
Application	Sgminer Project	Sgminer	All	All	All	All

References

Reference	Source	Link
Stratum: extract_sockaddr: Truncate overlong addresses rather than st… · luke-jr/bfgminer@c80ad85 · GitHub	CONFIRM	github.c
stratum: parse_reconnect(): treat pool-sent URL as untrusted. · sgminer-dev/sgminer@78cc408 · GitHub	CONFIRM	github.c
Stratum: extract_sockaddr: Truncate overlong addresses rather than st… · sgminer-dev/sgminer@b65574b · GitHub	CONFIRM	github.c
Full Disclosure: CVE-2014-4501 : Stack Overflow in Parsing client.reconnect Message of the Stratum Mining Protocol	FULLDISC	seclists.
Do some random sanity checking for stratum message parsing · ckolivas/cgminer@e1c5050 · GitHub	CONFIRM	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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**