



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 remote attackers to execute arbitrary code or cause a denial of service (crash) via crafted input to the CPUID instruction.

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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)