



CVE-2014-4502

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

Summary

CVE	CVE-2014-4502
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-23 14:55:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple heap-based buffer overflows in the parse_notify function in sgminer before 4.2.2, cgminer before 4.3.5, and BFGMiner before 3.10.0.0 allow remote attackers to execute arbitrary code or cause a denial of service (crash) via crafted data to the parse_notify function.

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

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	All	All	All	All
Application	Bfgminer	Bfgminer	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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Do some random sanity checking for stratum message parsing · ckolivas/cgminer@e1c5050 · GitHub	af854a3
Multiple Products 'parse_notify' Function Heap Based Buffer Overflow Vulnerabilities	af854a3
Bugfix: initiate_stratum: Ensure extranonce2 size is not negative (wh... · luke-jr/bfgminer@ff7f301 · GitHub	af854a3
Extranonce2 size not checked properly · Issue #258 · sgminer-dev/sgminer · GitHub	af854a3
Full Disclosure: CVE-2014-4502 : Invalid Handling of Length Parameter in Stratum mining.notify Message Leads to Heap Overflow	af854a3
Bugfix: initiate_stratum: Ensure extranonce2 size is not negative (wh... · sgminer-dev/sgminer@bac5831 · GitHub	af854a3
CVE Program record	CVE.OP
NVD vulnerability detail	NVD



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](#)