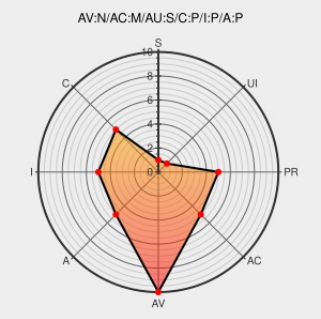
CVE-2014-6251

Published on: 10/24/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:54 PM UTC

CVE-2014-6251

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cpuminer from Cpuminer Project contain the following vulnerability:

Stack-based buffer overflow in CPUMiner before 2.4.1 allows remote attackers to have an unspecified impact by sending a mining.subscribe response with a large nonce2 length, then triggering the overflow with a mining.notify request.

CVE-2014-6251 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: CVE-2014-6251 : Stack Overflow in CPUMiner When Submitting Upstream Work	seclists.org text/html	FULLDISC 20141007 CVE-2014-6251 : Stack Overflow in CPUMiner When Submitting Upstream Work

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Cpuminer Project	Cpuminer	All	All	All	All

cpe:2.3:a:cpuminer_project:cpuminer:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→