

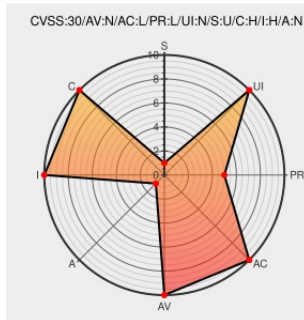


CVE-2017-16929

Published on: 12/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16929

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Claymore Dual Miner](#) from [Claymore Dual Miner Project](#) contain the following vulnerability:

The remote management interface on the Claymore Dual GPU miner 10.1 is vulnerable to an authenticated directory traversal vulnerability exploited by issuing a specially crafted request, allowing a remote attacker to read/write arbitrary files. This can be exploited via ../ sequences in the pathname to miner_file or miner_getfile.

CVE-2017-16929 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	NONE

CVE References

Description	Tags	Link
oss-security - CVE-2017-16930 - Claymore's Dual Ethereum Miner unauth stack buffer overflow in remote management interface	Mailing List www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2017/12/04/3

Claymore Dual ETH + DCR/SC/LBC/PASC GPU Miner - Stack Buffer Overflow / Path Traversal

Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

EXPLOIT-DB 43231

pub/pocs/cve-2017-16929 at master · tintinweb/pub · GitHub

Third Party Advisory

github.com

text/html

MISC
github.com/tintinweb/pub/tree/master/pocs/cve-2017-16929

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	Claymore Dual Miner Project	Claymore Dual Miner	10.1	All	All	All
Application	Claymore Dual Miner Project	Claymore Dual Miner	10.1	All	All	All
cpe:2.3:a:claymore_dual_miner_project:claymore_dual_miner:10.1:*:*:*:*:*:						
cpe:2.3:a:claymore_dual_miner_project:claymore_dual_miner:10.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE