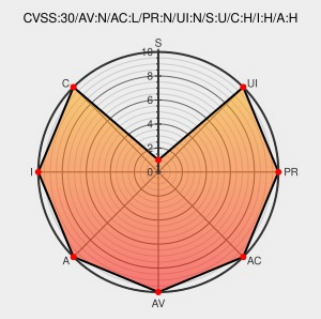
CVE-2017-16930

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

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

CVE-2017-16930

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 allows an unauthenticated remote attacker to execute arbitrary code due to a stack-based buffer overflow in the request handler. This can be exploited via a long API request that is mishandled during logging.

CVE-2017-16930 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
pub/pocs/cve-2017-16930 at master · tintinweb/pub · GitHub	Third Party Advisory github.com text/html	MISC github.com/tintinweb/pub/tree/master/pocs/cve-2017-16930

oss-security - CVE-2017-16930 - Claymore's Dual Ethereum Miner unauth stack buffer overflow in remote management interface	Mailing List Third Party Advisory 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

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

← Previous ID

Next ID→