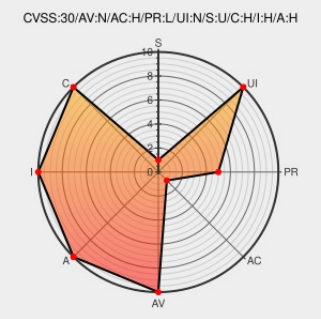
CVE-2018-1000049

Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000049

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



Certain versions of Claymore Dual Miner from Nanopool contain the following vulnerability:

Nanopool Claymore Dual Miner version 7.3 and earlier contains a remote code execution vulnerability by abusing the miner API. The flaw can be exploited only if the software is executed with read/write mode enabled.

CVE-2018-1000049 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

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
	raw.githubusercontent.com text/plain Inactive Link Not Archived	MISC raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2018/1000xxx/CVE-2018-1000049.json
Nanopool	packetstormsecurity.com	MISC packetstormsecurity.com/files/148578/Nanopool-Claymore-Dual-Miner-APIs-

Claymore Dual Miner APIs Remote Code Execution ≈ Packet Storm	text/html	Remote-Code-Execution.html
CVE-2018-1000049 Nanopool Claymore Dual Miner APIs RCE | Rapid7	www.rapid7.com text/html	MISC www.rapid7.com/db/modules/exploit/multi/misc/claymore_dual_miner_remote_manager_rce
Claymore Dual Miner Remote Code Execution	web.archive.org text/html Inactive Link Not Archived	MISC reversebrain.github.io/2018/02/01/Claymore-Dual-Miner-Remote-Code-Execution
Nanopool Claymore Dual Miner 7.3 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/147678/Nanopool-Claymore-Dual-Miner-7.3-Remote-Code-Execution.html
ReverseBrain na Twitterze: "PoC of Claymore Dual Miner Remote Code Execution… "	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/ReverseBrain/status/951850534985662464
Nanopool Claymore Dual Miner - APIs Remote Code Execution (Metasploit) - Multiple remote Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 45044
Claymore Dual Miner Remote Code Execution	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC reversebrain.github.io/2018/02/01/Claymore-Dual-Miner-Remote-Code-Execution/
Nanopool Claymore Dual Miner 7.3 - Remote Code Execution - Windows remote Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 44638

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nanopool	Claymore Dual Miner	All	All	All	All

cpe:2.3:a:nanopool:claymore_dual_miner:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→