



CVE-2020-6627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6627
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-06 15:15:00 UTC
Updated	2023-05-26 17:15:00 UTC
Description	The web-management application on Seagate Central NAS STCG2000300, STCG3000300, and STCG4000300 devices al

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Seagate	Stcg2000300	-	All	All	All
Operating System	Seagate	Stcg2000300 Firmware	-	All	All	All
Hardware	Seagate	Stcg3000300	-	All	All	All
Operating System	Seagate	Stcg3000300 Firmware	-	All	All	All
Hardware	Seagate	Stcg4000300	-	All	All	All
Operating System	Seagate	Stcg4000300 Firmware	-	All	All	All

References

Reference
403 Forbidden
Advisory Seagate Central Storage Remote Code Execution 0day – Pentest Blog
Seagate Central Storage 2015.0916 User Creation / Command Execution ≈ Packet Storm
Adding Seagate Central Storage SSH User Add (CVE-2020-6627) Module by EgeBalci · Pull Request #12844 · rapid7/metasploit-framework
CVE Program record
NVD vulnerability detail

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)