



CVE-2022-27224

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

Summary

CVE	CVE-2022-27224
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-09 15:15:00 UTC
Updated	2022-10-12 02:44:00 UTC
Description	An issue was discovered in Galleon NTS-6002-GPS 4.14.103-Galleon-NTS-6002.V12 4. An authenticated attacker can per

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Galsys	Nts-6002-gps	-	All	All	All
Operating System	Galsys	Nts-6002-gps Firmware	4.14.103-galleon-nts-6002.v12_4	All	All	All

References

Reference	Source
Galleon Download page Time Servers NTP Time Servers Synchronised Network Clocks Large Digital Wall Clocks Galleon Systems	M
An issue was discovered in Galleon NTS-6002-GPS > 4.14.103-Galleon-NTS-6002 V12-4 · GitHub	M
Galleon NTS-6002-GPS Command Injection vulnerability (CVE-2022-27224) Pen Test Partners	M
CVE Program record	C
NVD vulnerability detail	M

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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