



CVE-2019-9974

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

Summary

CVE	CVE-2019-9974
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-11 19:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	diag_tool.cgi on DASAN H660RM GPON routers with firmware 1.03-0022 lacks any authorization check, which allows remote attackers to execute arbitrary commands via the 'cmd' parameter.

Risk And Classification

Problem Types: CWE-306 | CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dasannetworks	H660rm	-	All	All	All
Hardware	Dasannetworks	H660rm	-	All	All	All
Operating System	Dasannetworks	H660rm Firmware	1.03-0022	All	All	All
Operating System	Dasannetworks	H660rm Firmware	1.03-0022	All	All	All

References

Reference
DASAN H660RM Information Disclosure / Hardcoded Key ≈ Packet Storm
diag_tool.cgi on DASAN H660RM devices with firmware 1.03-0022 allows spawning ping processes without any authorization leading to information disclosure
Bugtraq: Multiple vulnerabilities in DASAN H660RM GPON router firmware
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](#).

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

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