



CVE-2006-5704

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

Summary

CVE	CVE-2006-5704
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-04 01:07:00 UTC
Updated	2017-07-20 01:33:00 UTC
Description	HP NonStop Server G06.29, when running Standard Security T6533G06 before T6533G06^ABK, does not properly evaluate

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hp	Nonstop Server	g06.29	All	All	All
Hardware	Hp	Nonstop Server	g06.29	All	All	All

References

Reference	Source	Link
HP NonStop Server Unauthorized Directory Access Vulnerability	BID	www.security
IBM X-Force Exchange	XF	exchange.xfc
SecurityTracker.com Archives - HP NonStop Server Lets Local Users Access Restricted Files in Certain Cases	SECTrack	securitytracke
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.c
R-027: HP NonStop Server Running G06.29	CIAC	www.ciac.org
HP Technical Support, Help, and Troubleshooting HP® Customer Support	HP	www2.itrc.hp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)