



CVE-2007-1324

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

Summary

CVE	CVE-2007-1324
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-07 21:19:00 UTC
Updated	2017-07-29 01:30:00 UTC
Description	SnapGear 560, 585, 580, 640, 710, and 720 appliances before the 3.1.4u5 firmware allow remote attackers to cause a deni

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Snapgear	560	1.7.10_firmware	All	All	All
Hardware	Snapgear	560	1.7.8_firmware	All	All	All
Hardware	Snapgear	560	1.7.9_firmware	All	All	All
Hardware	Snapgear	560	1.8.4_firmware	All	All	All
Hardware	Snapgear	560	1.8.5_firmware	All	All	All
Hardware	Snapgear	560	1.8_firmware	All	All	All
Hardware	Snapgear	560	3.1.4u2	All	All	All
Hardware	Snapgear	560	1.7.10_firmware	All	All	All
Hardware	Snapgear	560	1.7.8_firmware	All	All	All
Hardware	Snapgear	560	1.7.9_firmware	All	All	All
Hardware	Snapgear	560	1.8.4_firmware	All	All	All
Hardware	Snapgear	560	1.8.5_firmware	All	All	All
Hardware	Snapgear	560	1.8_firmware	All	All	All
Hardware	Snapgear	560	3.1.4u2	All	All	All
Hardware	Snapgear	580	1.7.10_firmware	All	All	All
Hardware	Snapgear	580	1.7.8_firmware	All	All	All
Hardware	Snapgear	580	1.7.9_firmware	All	All	All

Hardware	Snapgear	580	1.8.4_firmware	All	All	All
Hardware	Snapgear	580	1.8.5_firmware	All	All	All
Hardware	Snapgear	580	1.8_firmware	All	All	All
Hardware	Snapgear	580	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	580	1.7.10_firmware	All	All	All
Hardware	Snapgear	580	1.7.8_firmware	All	All	All
Hardware	Snapgear	580	1.7.9_firmware	All	All	All
Hardware	Snapgear	580	1.8.4_firmware	All	All	All
Hardware	Snapgear	580	1.8.5_firmware	All	All	All
Hardware	Snapgear	580	1.8_firmware	All	All	All
Hardware	Snapgear	580	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	585	1.7.10_firmware	All	All	All
Hardware	Snapgear	585	1.7.8_firmware	All	All	All
Hardware	Snapgear	585	1.7.9_firmware	All	All	All
Hardware	Snapgear	585	1.8.4_firmware	All	All	All
Hardware	Snapgear	585	1.8.5_firmware	All	All	All
Hardware	Snapgear	585	1.8_firmware	All	All	All
Hardware	Snapgear	585	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	585	1.7.10_firmware	All	All	All
Hardware	Snapgear	585	1.7.8_firmware	All	All	All
Hardware	Snapgear	585	1.7.9_firmware	All	All	All
Hardware	Snapgear	585	1.8.4_firmware	All	All	All
Hardware	Snapgear	585	1.8.5_firmware	All	All	All
Hardware	Snapgear	585	1.8_firmware	All	All	All
Hardware	Snapgear	585	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	640	1.7.10_firmware	All	All	All
Hardware	Snapgear	640	1.7.8_firmware	All	All	All
Hardware	Snapgear	640	1.7.9_firmware	All	All	All
Hardware	Snapgear	640	1.8.4_firmware	All	All	All
Hardware	Snapgear	640	1.8.5_firmware	All	All	All
Hardware	Snapgear	640	1.8_firmware	All	All	All
Hardware	Snapgear	640	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	640	1.7.10_firmware	All	All	All
Hardware	Snapgear	640	1.7.8_firmware	All	All	All
Hardware	Snapgear	640	1.7.9_firmware	All	All	All

Hardware	Snapgear	640	1.8.4_firmware	All	All	All
Hardware	Snapgear	640	1.8.5_firmware	All	All	All
Hardware	Snapgear	640	1.8_firmware	All	All	All
Hardware	Snapgear	640	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	710	1.7.10_firmware	All	All	All
Hardware	Snapgear	710	1.7.8_firmware	All	All	All
Hardware	Snapgear	710	1.7.9_firmware	All	All	All
Hardware	Snapgear	710	1.8.4_firmware	All	All	All
Hardware	Snapgear	710	1.8.5_firmware	All	All	All
Hardware	Snapgear	710	1.8_firmware	All	All	All
Hardware	Snapgear	710	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	710	1.7.10_firmware	All	All	All
Hardware	Snapgear	710	1.7.8_firmware	All	All	All
Hardware	Snapgear	710	1.7.9_firmware	All	All	All
Hardware	Snapgear	710	1.8.4_firmware	All	All	All
Hardware	Snapgear	710	1.8.5_firmware	All	All	All
Hardware	Snapgear	710	1.8_firmware	All	All	All
Hardware	Snapgear	710	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	720	1.7.10_firmware	All	All	All
Hardware	Snapgear	720	1.7.8_firmware	All	All	All
Hardware	Snapgear	720	1.7.9_firmware	All	All	All
Hardware	Snapgear	720	1.8.4_firmware	All	All	All
Hardware	Snapgear	720	1.8.5_firmware	All	All	All
Hardware	Snapgear	720	1.8_firmware	All	All	All
Hardware	Snapgear	720	3.1.4u2_firmware	All	All	All
Hardware	Snapgear	720	1.7.10_firmware	All	All	All
Hardware	Snapgear	720	1.7.8_firmware	All	All	All
Hardware	Snapgear	720	1.7.9_firmware	All	All	All
Hardware	Snapgear	720	1.8.4_firmware	All	All	All
Hardware	Snapgear	720	1.8.5_firmware	All	All	All
Hardware	Snapgear	720	1.8_firmware	All	All	All
Hardware	Snapgear	720	3.1.4u2_firmware	All	All	All

References						
Reference	Source	Link	Tags			
SnapGear Packet Handling Denial of Service - Advisories - Secunia	SECUNIA	secunia.com				

IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
33864	OSVDB	osvdb.org	
SnapGear Unspecified Denial Of Service Vulnerability	BID	www.securityfocus.com	
CyberGuard: Premium Firewall / VPN Appliances	CONFIRM	www.cyberguard.info	Patch, Vendor Advisory
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report