



CVE-2011-2723

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

Summary

CVE	CVE-2011-2723
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-06 15:55:00 UTC
Updated	2023-02-13 01:20:00 UTC
Description	The skb_gro_header_slow function in include/linux/netdevice.h in the Linux kernel before 2.6.39.4, when Generic Receive Offload (GRO) is enabled, allows remote users to cause a denial of service (DoS) by sending a crafted packet, which triggers a kernel panic. This is a result of a race condition between the skb_gro_header_slow function and the skb_gro_header_fast function. The race condition occurs when the skb_gro_header_slow function is called while the skb_gro_header_fast function is still processing the packet. This results in the skb_gro_header_slow function seeing a partially processed packet, which causes it to crash. This vulnerability is present in the Linux kernel versions 2.6.39.4 and earlier.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
726552 – (CVE-2011-2723) CVE-2011-2723 kernel: gro: only reset frag0 when skb can be pulled	CONFIRM	bugzilla.r
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	HP	marc.info
oss-security - CVE request: kernel: gro: Only reset frag0 when skb can be pulled	MLIST	openwall
404: File not found	CONFIRM	www.ker
Linux Kernel Generic Receive Offload (GRO) CVE-2011-2723 Denial of Service Vulnerability	BID	www.sec
Linux Kernel skb_gro_header_slow() Bug Lets Remote Users Deny Service - SecurityTracker	SECTrack	securitytr
oss-security - Re: CVE request: kernel: gro: Only reset frag0 when skb can be pulled	MLIST	openwall
Support	REDHAT	www.red
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)