



CVE-2007-0251

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2007-0251
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-16 23:28:00 UTC
Updated	2018-10-16 16:32:00 UTC
Description	Integer underflow in the DecodeGRE function in src/decode.c in Snort 2.6.1.2 allows remote attackers to trigger dereferenci

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snort	Snort	2.6.1.2	All	All	All
Application	Snort	Snort	2.6.1.2	All	All	All

References

Reference	Source
32095	OSVDB
Calypix Your Simple and Powerful Network Security Solution	MISC
Snort GRE Packet Decoding Integer Underflow Vulnerability	BID
Just a moment...	CONFIR
SecurityFocus	BUGTRA
SecurityTracker.com Archives - Snort Integer Underflow in Processing the GRE Protocol May Let Remote Users Corrupt Log Files	SECTRA
SecurityReason - Snort 2.6.1.2 Integer Underflow Vulnerability	SREASC
33464	OSVDB
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

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