CVE-2007-0257

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-0257
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-16 23:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in the expand_stack function in grsecurity PaX allows local users to gain privileges via unspecified

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: NVD-CWE-Other | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grsecurity	Grsecurity Kernel Patch	1.9.4	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.0.1	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.0.2	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.0	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.1	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.2	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.3	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.4	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.5	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.6	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.7	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.1.8	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
PaX expand_stack() Lets Local Users Gain Root Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108
grsecurity "expand_stack()" Privilege Escalation Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108
Grsecurity Kernel PaX Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661108
grsecurity	af854a3a-2127-422b-91ae-364da2661108
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108
Pre-advisory: Grsecurity Kernel PaX - Local root vulnerability - Digital Armaments for Intelligence	af854a3a-2127-422b-91ae-364da2661108
News - Digital Armaments for Intelligence	af854a3a-2127-422b-91ae-364da2661108
osvdb.org/32727	af854a3a-2127-422b-91ae-364da2661108
grsecurity forums • View topic - Local root in expand_stack()?	af854a3a-2127-422b-91ae-364da2661108
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108
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.