



CVE-2006-1168

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2006-1168
State	PUBLISHED
Assigner	sgi
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-14 20:04:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The decompress function in compress42.c in (1) ncompress 4.2.4 and (2) liblz allows remote attackers to cause a denial of service (CPU consumption) by sending a large number of compressed blocks.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.098140000 probability, percentile 0.929860000 (date 2026-04-21)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Ncompress	Ncompress	4.2.4	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
Advisories - Mandriva Linux				af854a3a-2127-42f		
Support				af854a3a-2127-42f		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-2127-42f		
Avaya Products ncompress Buffer Overflow Vulnerability - Advisories - Secunia				af854a3a-2127-42f		
ASA-2006-226 (RHSA-2006-0663)				af854a3a-2127-42f		
patches.sgi.com/support/free/security/advisories/20060901-01-P.asc				af854a3a-2127-42f		
ncompress: Buffer Underflow — Gentoo Linux Documentation				af854a3a-2127-42f		
Security Announcement				af854a3a-2127-42f		
Gentoo update for ncompress - Advisories - Secunia				af854a3a-2127-42f		
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-42f		
SecurityTracker.com Archives - ncompress Buffer Overflow in decompress() Lets Remote Users Execute Arbitrary Code				af854a3a-2127-42f		
Red Hat Customer Portal				af854a3a-2127-42f		
Debian -- Security Information -- DSA-1149-1 ncompress				af854a3a-2127-42f		
Secunia - Advisories - ncompress "decompress()" Buffer Overflow Vulnerability				af854a3a-2127-42f		
Gentoo Bug 141728 - {app-arch/ncompress dev-libs/liblzw} 4.2.4 security flaw in decompression				af854a3a-2127-42f		
Secunia - Advisories - Mandriva update for ncompress				af854a3a-2127-42f		
Red Hat update for ncompress - Advisories - Secunia				af854a3a-2127-42f		
NCompress Decompress Buffer Underflow Vulnerability				af854a3a-2127-42f		
Repository / Oval Repository				af854a3a-2127-42f		
Bug 728536 – CVE-2006-1168 busybox: uncompress buffer underflow				af854a3a-2127-42f		
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia				af854a3a-2127-42f		
ASA-2012-117 (RHSA-2012-0308)				af854a3a-2127-42f		
Support / Security / Advisories / / MDVSA-2012:129 Mandriva				af854a3a-2127-42f		
IBM X-Force Exchange				af854a3a-2127-42f		
Secunia - Advisories - Debian update for ncompress				af854a3a-2127-42f		
CVE Program record				CVE.ORG		
NVD vulnerability detail				NVD		

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.
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](#)