



CVE-2003-0848

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

Summary

CVE	CVE-2003-0848
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-11-17 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Heap-based buffer overflow in main.c of slocate 2.6, and possibly other versions, may allow local users to gain privileges via a crafted file name.

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/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	Slocate	Slocate	2.1	All	All	All

Application	Slocate	Slocate	2.2	All	All	All
Application	Slocate	Slocate	2.3	All	All	All
Application	Slocate	Slocate	2.4	All	All	All
Application	Slocate	Slocate	2.5	All	All	All
Application	Slocate	Slocate	2.6	All	All	All

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

References			
Reference	Source	Link	
Secunia - Advisories - slocate User Database Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
patches.sgi.com/support/free/security/advisories/20040201-01-U.asc	af854a3a-2127-422b-91ae-364da2661108	patches.sg	
www.trustix.org/errata/misc/2004/TSL-2004-0005-slocate.asc.txt	af854a3a-2127-422b-91ae-364da2661108	www.trustix	
Red Hat -- Linux, Embedded Linux and Open Source Solutions	af854a3a-2127-422b-91ae-364da2661108	www.redhat	
Secunia - Advisories - Debian update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat	
'SA-20031006 slocate vulnerability' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
Advisories - Mandriva	af854a3a-2127-422b-91ae-364da2661108	www.mandr	
Secunia - Advisories - Fedora update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.	
Secunia - Advisories - Mandrake update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
patches.sgi.com/support/free/security/advisories/20040202-01-U.asc	af854a3a-2127-422b-91ae-364da2661108	patches.sg	
www.ebitech.sk/patrik/SA/SA-20031006-A.txt	af854a3a-2127-422b-91ae-364da2661108	www.ebitech	
Secunia - Advisories - Red Hat update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
'SA-20031006 slocate buffer overflow - exploitation proof' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
Secunia - Advisories - Trustix update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
Debian -- Security Information -- DSA-428-1 slocate	af854a3a-2127-422b-91ae-364da2661108	www.debian	
ftp.sco.com/pub/updates/OpenLinux/3.1.1/Workstation/CSSA-2004-001.0/CSSA-...	af854a3a-2127-422b-91ae-364da2661108	ftp.sco.com	
www.ebitech.sk/patrik/SA/SA-20031006.txt	af854a3a-2127-422b-91ae-364da2661108	www.ebitech	
Secunia - Advisories - Sun Cobalt update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
Secunia - Advisories - Red Hat update for slocate	af854a3a-2127-422b-91ae-364da2661108	secunia.co	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecu	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecu	
CVE Program record	CVE.ORG	www.cve.o	
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](#)