



CVE-2007-3919

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

Summary

CVE	CVE-2007-3919
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-28 17:08:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	(1) xenbaked and (2) xenmon.py in Xen 3.1 and earlier allow local users to truncate arbitrary files via a symlink attack on /tr

Risk And Classification

Primary CVSS: v2.0 6 from nvd@nist.gov

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

Problem Types: CWE-59 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	4.0	All	alpha	All

Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All
Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All
Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All
Application	Xensource Inc	Xen	3.0.3_0_1	All	All	All
Application	Xensource Inc	Xen	3.0.3_0_3	All	All	All

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

References						
Reference					Source	
Fedora update for xen - Advisories - Secunia					af854a3a-2127-422b-9	
Xen 'xenmon.py' and 'xenbaked' Insecure Temporary File Creation Vulnerability					af854a3a-2127-422b-9	
[SECURITY] Fedora Core 6 Update: xen-3.0.3-13.fc6					af854a3a-2127-422b-9	
Xen Insecure Temporary File Lets Local Users Truncate Files - SecurityTracker					af854a3a-2127-422b-9	
Debian -- Security Information -- DSA-1395-1 xen-utils					af854a3a-2127-422b-9	
IBM X-Force Exchange					af854a3a-2127-422b-9	
Webmail- OVH					af854a3a-2127-422b-9	
[SECURITY] Fedora 7 Update: xen-3.1.0-8.fc7					af854a3a-2127-422b-9	
Mandriva update for xen - Advisories - Secunia					af854a3a-2127-422b-9	
Red Hat update for xen - Advisories - Secunia					af854a3a-2127-422b-9	
Xen "xenbaked" Insecure Temporary Files - Advisories - Secunia					af854a3a-2127-422b-9	
Support / Security / Advisories / / MDKSA-2007:203 Mandriva					af854a3a-2127-422b-9	
#447795 - xen-utils-3.0.3-1: [CVE-2007-3919] xenmon.py / xenbaked insecure file accesss - Debian Bug report logs					af854a3a-2127-422b-9	
osvdb.org/41343					af854a3a-2127-422b-9	
Repository / Oval Repository					af854a3a-2127-422b-9	
osvdb.org/41342					af854a3a-2127-422b-9	
Debian update for xen utils - Advisories - Secunia					af854a3a-2127-422b-9	

Debian update for xentools - Advisories - Security	af854a3a-2127-422b-9
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-9
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-11-01	Mark J Cox	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/

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](#)