



CVE-2007-4752

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-4752
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-12 01:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11

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

Problem Types: CWE-20 | 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	Openbsd	Openssh	4.0	All	All	All

Application	Openbsd	Openssh	4.0p1	All	All	All
Application	Openbsd	Openssh	4.1	All	All	All
Application	Openbsd	Openssh	4.1p1	All	All	All
Application	Openbsd	Openssh	4.2	All	All	All
Application	Openbsd	Openssh	4.2p1	All	All	All
Application	Openbsd	Openssh	4.3	All	All	All
Application	Openbsd	Openssh	4.3p1	All	All	All
Application	Openbsd	Openssh	4.3p2	All	All	All
Application	Openbsd	Openssh	4.4	All	All	All
Application	Openbsd	Openssh	4.4p1	All	All	All
Application	Openbsd	Openssh	4.5	All	All	All
Application	Openbsd	Openssh	All	All	All	All

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

References	
Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
Red Hat Update for Tampered OpenSSH Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854
OpenSSH X11 Cookie Local Authentication Bypass Vulnerability	af854
Bug 280471 – openssh falls back to the trusted x11 cookie if generation of an untrusted cookie fails [FC6]	af854
[#RPL-1706] openssh uses a trusted X11cookie if creation of an untrusted cookie fails CVE-2007-4752 - rPath Issue Tracking System	af854
SecurityReason - OpenSSH uses a trusted X11 cookie if creation of an untrusted cookie fails	af854
IBM X-Force Exchange	af854
Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854
Avaya Products Red Hat Tampered OpenSSH Packages - Advisories - Community	af854
About Security Update 2008-002	af854
Support	af854
ASA-2008-399 (RHSA-2008-0855)	af854
USN-566-1: OpenSSH vulnerability Ubuntu	af854
[security-announce] SUSE Security Summary Report SUSE-SR:2007:022	af854
Repository / Oval Repository	af854
SUSE Update for Multiple Packages - Advisories - Secunia	af854
APPLE-SA-2008-03-18 Security Update 2008-002	af854
Centos Linux Documentation - OpenSSH: Security bugs	af854

Gentoo Linux Documentation -- OpenSSH: Security bypass	af854
[SECURITY] Fedora Core 6 Update: openssh-4.3p2-25.fc6	af854
Support / Security / Advisories / / MDKSA-2007:236 Mandriva	af854
www.openssh.com/txt/release-4.7	af854
Debian -- Security Information -- DSA-1576-1 openssh	af854
Webmail - OVH	af854
h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp	af854
SecurityFocus	af854
Debian update for openssh - Secunia Advisories - Vulnerability Information - Secunia.com	af854
Gentoo Bug 191321 - net-misc/openssh <4.7 X11 cookie privelege escalation (CVE-2007-4752)	af854
Repository / Oval Repository	af854
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854
SecurityFocus	af854
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2008-08-28	Mark J Cox	This issue did not affect the OpenSSH packages as distributed with Red Hat Enterprise Linux 2.

There are currently no legacy QID mappings associated with this CVE.