



CVE-2015-2157

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

Summary

CVE	CVE-2015-2157
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-27 14:59:00 UTC
Updated	2019-03-21 17:04:00 UTC
Description	The (1) ssh2_load_userkey and (2) ssh2_save_userkey functions in PuTTY 0.51 through 0.63 do not properly wipe SSH-2

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Putty	Putty	0.51	All	All	All
Application	Putty	Putty	0.52	All	All	All
Application	Putty	Putty	0.53b	All	All	All
Application	Putty	Putty	0.54	All	All	All
Application	Putty	Putty	0.55	All	All	All
Application	Putty	Putty	0.56	All	All	All
Application	Putty	Putty	0.57	All	All	All

Application	Putty	Putty	0.58	All	All	All
Application	Putty	Putty	0.59	All	All	All
Application	Putty	Putty	0.60	All	All	All
Application	Putty	Putty	0.61	All	All	All
Application	Putty	Putty	0.62	All	All	All
Application	Putty	Putty	0.63	All	All	All
Application	Putty	Putty	0.51	All	All	All
Application	Putty	Putty	0.52	All	All	All
Application	Putty	Putty	0.53b	All	All	All
Application	Putty	Putty	0.54	All	All	All
Application	Putty	Putty	0.55	All	All	All
Application	Putty	Putty	0.56	All	All	All
Application	Putty	Putty	0.57	All	All	All
Application	Putty	Putty	0.58	All	All	All
Application	Putty	Putty	0.59	All	All	All
Application	Putty	Putty	0.60	All	All	All
Application	Putty	Putty	0.61	All	All	All
Application	Putty	Putty	0.62	All	All	All
Application	Putty	Putty	0.63	All	All	All
Application	Simon Tatham	Putty	0.53	All	All	All
Application	Simon Tatham	Putty	0.53	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 21 Update: putty-0.64-1.fc21	FEDORA	lists.fedoraproject.org	
PuTTY vulnerability private-key-not-wiped-2	CONFIRM	www.chiark.greenend.org.uk	Patc
PuTTY Change Log	CONFIRM	www.chiark.greenend.org.uk	Patc
Debian -- Security Information -- DSA-3190-1 putty	DEBIAN	www.debian.org	
openSUSE-SU-2015:0474-1: moderate: Security update for putty	SUSE	lists.opensuse.org	
oss-security - CVE Request: PuTTY fails to clear private key information from memory	MLIST	www.openwall.com	
[SECURITY] Fedora 22 Update: putty-0.64-1.fc22	FEDORA	lists.fedoraproject.org	
oss-security - Re: CVE Request: PuTTY fails to clear private key information from memory	MLIST	www.openwall.com	
[SECURITY] Fedora 20 Update: putty-0.64-1.fc20	FEDORA	lists.fedoraproject.org	
PuTTY CVE-2015-2157 Local Information Disclosure Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canc

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)