



# CVE-2017-6542

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-6542
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-27 17:59:00 UTC
<b>Updated</b>	2023-11-07 02:49:00 UTC
<b>Description</b>	The ssh_agent_channel_data function in PuTTY before 0.68 allows remote attackers to have unspecified impact via a large

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Leap</a>	42.1	All	All	All
Application	<a href="#">Putty</a>	<a href="#">Putty</a>	All	All	All	All

## References

Reference	Source
PuTTY < 0.68 - 'ssh_agent_channel_data' Integer Overflow Heap Corruption - Linux dos Exploit	EXPLOIT
openSUSE-SU-2017:0741-1: moderate: Security update for putty	SUSE
PuTTY vulnerability vuln-agent-fwd-overflow	CONFIR
git.tartarus.org Git - simon/putty.git/commitdiff	
PuTTY 'ssh_agent_channel_data()' Function Integer Overflow Vulnerability	BID
PuTTY: Buffer overflow (GLSA 201703-03) — Gentoo security	GENTOO
PuTTY Integer Overflow in ssh_agent_channel_data Lets Local Users Gain Elevated Privileges or Deny Service - SecurityTracker	SECTRA
git.tartarus.org Git - simon/putty.git/commitdiff	CONFIR
FileZilla: Buffer overflow (GLSA 201706-09) — Gentoo security	GENTOO

CVE Program record

CVE.ORG

NVD vulnerability detail

NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710495](#) Gentoo Linux PuTTY Buffer overflow Vulnerability (GLSA 201703-03)

[710542](#) Gentoo Linux FileZilla Buffer overflow Vulnerability (GLSA 201706-09)

© [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](#)