CVE-2017-6542

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-6542
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-27 17:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	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	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse Project	Leap	42.1	All	All	All
Operating System	Opensuse Project	Leap	42.1	All	All	All
Application	Putty	Putty	All	All	All	All

References

Reference	Source
PuTTY < 0.68 - 'ssh_agent_channel_data' Integer Overflow Heap Corruption - Linux dos Exploit	EXPLOI
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.OR
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)