



CVE-2019-9898

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-9898
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	Potential recycling of random numbers used in cryptography exists within PuTTY before 0.71.

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Application	Putty	Putty	All	All	All	All
Application	Putty	Putty	All	All	All	All

References

Reference	Source	Link
SECURITY ID: A-1762-11 putty security update	MLIST	lists.debian.org

[SECURITY] [DSA 4423-1] putty security update	MISC	lists.debian.org
www.chiark.greenend.org.uk/~sgtatham/putty/changes.html	MISC	www.chiark.greenend.org.uk
[SECURITY] Fedora 29 Update: putty-0.71-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2019:1123-1: moderate: Security update f	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2019:1113-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] Fedora 29 Update: putty-0.71-1.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2019-9898 PuTTY Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Debian -- Security Information -- DSA-4423-1 putty	DEBIAN	www.debian.org
Bugtraq: [SECURITY] [DSA 4423-1] putty security update	BUGTRAQ	seclists.org
NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 28 Update: putty-0.71-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 28 Update: putty-0.71-1.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
PuTTY CVE-2019-9898 Security Weakness	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500552](#) Alpine Linux Security Update for putty

[504322](#) Alpine Linux Security Update for putty

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report