



# CVE-2020-14002

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

## Summary

<b>CVE</b>	CVE-2020-14002
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-29 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	PuTTY 0.68 through 0.73 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This a

## Risk And Classification

### Problem Types: CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Unified Manager Core Package</a>	-	All	All	All
Application	<a href="#">Putty</a>	<a href="#">Putty</a>	All	All	All	All

## References

Reference	Source	Link	T
[SECURITY] Fedora 32 Update: putty-0.74-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	
[SECURITY] Fedora 31 Update: putty-0.74-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	
CVE-2020-14002 PuTTY Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
<a href="#">www.chiark.greenend.org.uk/~sgtatham/putty/changes.html</a>	MISC	<a href="#">www.chiark.greenend.org.uk</a>	F
[SECURITY] Fedora 32 Update: putty-0.74-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
Detail en : FZI Forschungszentrum Informatik	MISC	<a href="#">www.fzi.de</a>	T
[SECURITY] Fedora 31 Update: putty-0.74-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
The PuTTY-announce Archives	MISC	<a href="#">lists.tartarus.org</a>	T
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	c
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	c

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

375441 Putty Multiple Security Vulnerabilities

500554 Alpine Linux Security Update for putty

504324 Alpine Linux Security Update for putty

© [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](#)**