



# CVE-2017-18594

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-18594
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-08-29 00:15:00 UTC
<b>Updated</b>	2019-09-26 12:15:00 UTC
<b>Description</b>	nse_libssh2.cc in Nmap 7.70 is subject to a denial of service condition due to a double free when an SSH connection fails, ,

## Risk And Classification

**Problem Types:** CWE-415

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Nmap</a>	<a href="#">Nmap</a>	7.70	All	All	All
Application	<a href="#">Nmap</a>	<a href="#">Nmap</a>	7.70	All	All	All

## References

Reference	Source	Link
Avoid a crash (double-free) when SSH connection fails · nmap/nmap@350bbe0 · GitHub	MISC	<a href="#">github.com</a>
Nmap Announce: Nmap Defcon Release! 80+ improvements include new NSE scripts/libs, new Npcap, etc.	MISC	<a href="#">seclists.org</a>
NMAP crash with ssh-auth-methods.nse (patch included) · Issue #1077 · nmap/nmap · GitHub	MISC	<a href="#">github.com</a>
Nmap Development: Crash in libssh with certain SSH scripts	MISC	<a href="#">seclists.org</a>
Research/Nmap&libsshDF at master · AMatchandaHaystack/Research · GitHub	MISC	<a href="#">github.com</a>
[security-announce] openSUSE-SU-2019:2198-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
Crash in libssh when port 22 response is unexpected · Issue #1227 · nmap/nmap · GitHub	MISC	<a href="#">github.com</a>
[security-announce] openSUSE-SU-2019:2200-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

500431 Alpine Linux Security Update for nmap

504194 Alpine Linux Security Update for nmap

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

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