



CVE-2016-8858

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

Summary

CVE	CVE-2016-8858
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-09 11:59:00 UTC
Updated	2023-11-07 02:36:00 UTC
Description	** DISPUTED ** The <code>kex_input_kexinit</code> function in <code>kex.c</code> in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to ca

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	6.8	All	All	All
Application	Openbsd	Openssh	6.9	All	All	All
Application	Openbsd	Openssh	7.0	All	All	All
Application	Openbsd	Openssh	7.1	All	All	All
Application	Openbsd	Openssh	7.2	All	All	All
Application	Openbsd	Openssh	7.3	All	All	All
Application	Openbsd	Openssh	6.8	All	All	All
Application	Openbsd	Openssh	6.9	All	All	All
Application	Openbsd	Openssh	7.0	All	All	All
Application	Openbsd	Openssh	7.1	All	All	All
Application	Openbsd	Openssh	7.2	All	All	All
Application	Openbsd	Openssh	7.3	All	All	All

References

Reference

- oss-security - Re: Re: CVE Request: OpenSSH: Memory exhaustion issue found in OpenSSH
- OpenSSH 'ssh/kex.c' Denial of Service Vulnerability

[src/usr.bin/ssh/kex.c - diff - 1.127](#)

[Bug 1384860 – CVE-2016-8858 openssh: Memory exhaustion due to unregistered KEXINIT handler after receiving message](#)

[OpenSSH: Multiple vulnerabilities \(GLSA 201612-18\) — Gentoo security](#)

[ftp.openbsd.org/pub/OpenBSD/patches/6.0/common/013_ssh_kexinit.patch.sig](#)

[FreeBSD-SA-16:33](#)

[upstream commit · openssh/openssh-portable@ec165c3 · GitHub](#)

[OpenSSH Key Exchange Initialization Bug in kex_input_kexinit\(\) Lets Remote Users Consume Excessive Memory Resources - SecurityTrack](#)

[oss-security - CVE Request: OpenSSH: Memory exhaustion issue found in OpenSSH](#)

[CVE-2016-8858 OpenSSH Vulnerability in NetApp Products | NetApp Product Security](#)

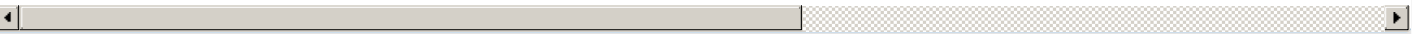
[cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf](#)

[Exploit not working in 6.6.p1 · Issue #1 · dag-erling/kexkill · GitHub](#)

[src/usr.bin/ssh/kex.c - view - 1.127](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

© [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](#)