



# CVE-2016-10012

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

## Summary

<b>CVE</b>	CVE-2016-10012
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-01-05 02:59:00 UTC
<b>Updated</b>	2023-11-07 02:29:00 UTC
<b>Description</b>	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not e

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference
[SECURITY] [DLA 1500-1] openssh security update
<a href="http://www.openssh.com/txt/release-7.4">www.openssh.com/txt/release-7.4</a>
<a href="http://support.f5.com/csp/article/K62201745">support.f5.com/csp/article/K62201745</a>
Document Display   HPE Support Center
oss-security - Announce: OpenSSH 7.4 released
OpenSSH Multiple Flaws Let Remote Authenticated Users Gain Elevated Privileges and Local Privileged Users Obtain Host Private Keys - Se
<a href="http://cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf">cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf</a>
The Slackware Linux Project: Slackware Security Advisories
myF5
Remove support for pre-authentication compression. Doing compression · openbsd/src@3095060 · GitHub
January 2017 OpenSSH Vulnerabilities in NetApp Products   NetApp Product Security
Red Hat Customer Portal
OpenSSH CVE-2016-10012 Security Bypass Vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500484](#) Alpine Linux Security Update for openssh

[504243](#) Alpine Linux Security Update for openssh

[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](#)**