



# CVE-2016-1231

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

## Summary

<b>CVE</b>	CVE-2016-1231
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-01-12 20:59:00 UTC
<b>Updated</b>	2016-06-15 16:48:00 UTC
<b>Description</b>	Directory traversal vulnerability in the HTTP file-serving module (mod_http_files) in Prosody 0.9.x before 0.9.9 allows remot

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.0	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.1	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.2	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.3	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.4	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.5	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.6	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.7	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.8	All	All	All

Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.0	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.1	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.2	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.3	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.4	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.5	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.6	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.7	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	0.9.8	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 23 Update: prosody-0.9.9-2.fc23	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Prosody 0.9.9 security release - Prosodical Thoughts	CONFIRM	<a href="https://blog.prosody.im">blog.prosody.im</a>	Patch,
oss-security - CVE-2016-1231, CVE-2016-1232: Prosody XMPP server multiple vulnerabilities	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
Debian -- Security Information -- DSA-3439-1 prosody	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 22 Update: prosody-0.9.9-2.fc22	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Prosody security advisory 2016/01/08 - 1	CONFIRM	<a href="https://prosody.im">prosody.im</a>	Vendc
#520 mod_http_files allows access outside of http_files_dir (closed) - Prosody IM Issue Tracker	CONFIRM	<a href="https://prosody.im">prosody.im</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)