



# CVE-2021-32921

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-32921
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-13 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	An issue was discovered in Prosody before 0.11.9. It does not use a constant-time algorithm for comparing certain secret s

## Risk And Classification

**Problem Types:** CWE-362

## 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>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Lua</a>	<a href="#">Lua</a>	All	All	All	All
Application	<a href="#">Prosody</a>	<a href="#">Prosody</a>	All	All	All	All

## References

Reference	Source	Link	Tag
[SECURITY] Fedora 34 Update: prosody-0.11.9-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Prosody 0.11.9 released   Prosodical Thoughts	MISC	<a href="https://blog.prosody.im">blog.prosody.im</a>	
[SECURITY] Fedora 33 Update: prosody-0.11.9-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
oss-security - Prosody XMPP server advisory 2021-05-12 (multiple vulnerabilities)	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
Debian -- Security Information -- DSA-4916-1 prosody	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 34 Update: prosody-0.11.9-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 32 Update: prosody-0.11.9-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 2687-2] prosody regression update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	

[SECURITY] Fedora 32 Update: prosody-0.11.9-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 2687-1] prosody security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
oss-security - Re: Prosody XMPP server advisory 2021-05-12 (multiple vulnerabilities)	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
[SECURITY] Fedora 33 Update: prosody-0.11.9-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Prosody IM: Multiple vulnerabilities (GLSA 202105-15) — Gentoo security	MISC	<a href="https://security.gentoo.org">security.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [178602](#) Debian Security Update for prosody (DSA 4916-1)
- [178674](#) Debian Security Update for prosody (DLA 2687-1)
- [178678](#) Debian Security Update for prosody (DLA 2687-2)
- [180414](#) Debian Security Update for prosody (CVE-2021-32921)
- [281156](#) Fedora Security Update for prosody (FEDORA-2021-498be8f560)
- [281157](#) Fedora Security Update for prosody (FEDORA-2021-b5d8c6d086)
- [281158](#) Fedora Security Update for prosody (FEDORA-2021-a33f6e36e1)
- [501226](#) Alpine Linux Security Update for prosody
- [690138](#) Free Berkeley Software Distribution (FreeBSD) Security Update for prosody (fc75570a-b417-11eb-a23d-c7ab331fd711)
- [710569](#) Gentoo Linux Prosody IM Multiple Vulnerabilities (GLSA 202105-15)

© [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](#)