



CVE-2014-2745

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

Summary

CVE	CVE-2014-2745
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-11 01:55:00 UTC
Updated	2014-04-19 04:48:00 UTC
Description	Prosody before 0.9.4 does not properly restrict the processing of compressed XML elements, which allows remote attacker:

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Prosody	Prosody	0.1.0	All	All	All
Application	Prosody	Prosody	0.2.0	All	All	All
Application	Prosody	Prosody	0.3.0	All	All	All
Application	Prosody	Prosody	0.4.0	All	All	All
Application	Prosody	Prosody	0.4.1	All	All	All
Application	Prosody	Prosody	0.4.2	All	All	All
Application	Prosody	Prosody	0.5.0	All	All	All
Application	Prosody	Prosody	0.5.1	All	All	All
Application	Prosody	Prosody	0.5.2	All	All	All
Application	Prosody	Prosody	0.6.0	All	All	All
Application	Prosody	Prosody	0.6.1	All	All	All
Application	Prosody	Prosody	0.6.2	All	All	All
Application	Prosody	Prosody	0.7.0	All	All	All
Application	Prosody	Prosody	0.8.0	All	All	All
Application	Prosody	Prosody	0.8.1	All	All	All
Application	Prosody	Prosody	0.8.2	All	All	All
Application	Prosody	Prosody	0.9.0	All	All	All

Application	Prosody	Prosody	0.9.1	All	All	All
Application	Prosody	Prosody	0.9.2	All	All	All
Application	Prosody	Prosody	All	All	All	All
Application	Prosody	Prosody	0.1.0	All	All	All
Application	Prosody	Prosody	0.2.0	All	All	All
Application	Prosody	Prosody	0.3.0	All	All	All
Application	Prosody	Prosody	0.4.0	All	All	All
Application	Prosody	Prosody	0.4.1	All	All	All
Application	Prosody	Prosody	0.4.2	All	All	All
Application	Prosody	Prosody	0.5.0	All	All	All
Application	Prosody	Prosody	0.5.1	All	All	All
Application	Prosody	Prosody	0.5.2	All	All	All
Application	Prosody	Prosody	0.6.0	All	All	All
Application	Prosody	Prosody	0.6.1	All	All	All
Application	Prosody	Prosody	0.6.2	All	All	All
Application	Prosody	Prosody	0.7.0	All	All	All
Application	Prosody	Prosody	0.8.0	All	All	All
Application	Prosody	Prosody	0.8.1	All	All	All
Application	Prosody	Prosody	0.8.2	All	All	All
Application	Prosody	Prosody	0.9.0	All	All	All
Application	Prosody	Prosody	0.9.1	All	All	All
Application	Prosody	Prosody	0.9.2	All	All	All

References

Reference

[oss-security - Re: Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Layer Compression](#)

[Debian -- Security Information -- DSA-2895-1 prosody](#)

[Prosody IM 0.9: revision 1107d66d2ab2: util.xmppstream: Implement stanza size limiting, default limit 10MB](#)

[Uncontrolled Resource Consumption with XMPP-Layer Compression – The XMPP Standards Foundation](#)

[oss-security - Re: \(Openfire M-Link Metronome Prosody Tigase\) Possible CVE Request: Uncontrolled Resource Consumption with XMPP-Lay](#)

[Prosody 0.9.4 released - Prosodical Thoughts](#)

[Security Advisory SA57710 - Debian update for prosody - Secunia](#)

[Prosody IM 0.9: revision a97591d2e1ad: portmanager: Make maximum read size configurable, and default to 4KB](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

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](#)