



CVE-2016-0756

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

Summary

CVE	CVE-2016-0756
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-29 20:59:00 UTC
Updated	2016-12-06 03:05:00 UTC
Description	The generate_dialback function in the mod_dialback module in Prosody before 0.9.10 does not properly separate fields wh

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Prosody	Prosody	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 23 Update: prosody-0.9.10-1.fc23	FEDORA	lists.fedoraproject.org
oss-security - CVE-2016-0756: Prosody XMPP server: insecure dialback key generation/validation algorithm	MLIST	www.openwall.com/lists/oss-security
#596 Dialback key generation in 0.9 allows servers to impersonate to suffices (closed) - Prosody IM Issue Tracker	CONFIRM	prosody.im
Debian -- Security Information -- DSA-3463-1 prosody	DEBIAN	www.debian.org/security
Prosody 0.9.10 released - Prosodical Thoughts	CONFIRM	blog.prosody.im
Prosody XMPP Server CVE-2016-0756 Security Bypass Vulnerability	BID	www.securityfocus.com/bid/78482
[SECURITY] Fedora 22 Update: prosody-0.9.10-1.fc22	FEDORA	lists.fedoraproject.org
Prosody security advisory 2016/01/08 - 1	CONFIRM	prosody.im
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)