



CVE-2016-7142

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

Summary

CVE	CVE-2016-7142
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-26 15:59:00 UTC
Updated	2020-09-14 12:33:00 UTC
Description	The m_sasl module in InspIRCd before 2.0.23, when used with a service that supports SASL_EXTERNAL authentication, a

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Inspircd	Inspircd	All	All	All	All

References

Reference	Source	Link
InspIRCd - v2.0.23 released!	CONFIRM	www.inspircd.org
oss-security - CVE ID request: certificate spoofing through crafted SASL message in inspircd, charybdis	MLIST	www.openwall.com
Debian -- Security Information -- DSA-3662-1 inspircd	DEBIAN	www.debian.org
m_sasl: don't allow AUTHENTICATE with mechanisms with a space · inspircd/inspircd@74fafb7 · GitHub	CONFIRM	github.com
oss-security - Re: CVE ID request: certificate spoofing through crafted SASL message in inspircd, charybdis	MLIST	www.openwall.com
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)