CVE-2015-3026

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3026
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-29 20:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Icecast before 2.4.2, when a stream_auth handler is defined for URL authentication, allows remote attackers to cause a der

Risk And Classification

Problem Types: NVD-CWE-Other

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
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Xiph	Icecast	All	All	All	All

References

Reference
oss-security - CVE Request for Icecast 2.3.3, 2.4.0, 2.4.1, fixed in 2.4.2
trac.xiph.org/changeset/27abfbbd688df3e3077b535997330aa06603250f/icecast-se...
Malformed Request
[SECURITY] Fedora 22 Update: icecast-2.4.2-1.fc22
#782120 - icecast2: icecast can be remotely killed by anyone if using <authentication type="url"> and stream_auth option (CVE-2015-3026) - I
[Icecast-dev] Icecast 2.4.2 - security release
oss-security - Re: CVE Request for Icecast 2.3.3, 2.4.0, 2.4.1, fixed in 2.4.2

[SECURITY] Fedora 23 Update: icecast-2.4.2-1.fc23
openSUSE-SU-2015:0728-1: moderate: Security update for icecast
Gentoo Security
#2191 (Icecast can be crashed remotely if stream_auth is enabled.) – Xiph
[SECURITY] Fedora 21 Update: icecast-2.4.2-1.fc21
Debian -- Security Information -- DSA-3239-1 icecast2
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.