



# CVE-2018-18820

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

## Summary

<b>CVE</b>	CVE-2018-18820
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-05 19:29:00 UTC
<b>Updated</b>	2019-01-23 18:28:00 UTC
<b>Description</b>	A buffer overflow was discovered in the URL-authentication backend of the Icecast before 2.4.4. If the backend is enabled,

## Risk And Classification

**Problem Types:** CWE-119

## 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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Xiph</a>	<a href="#">Icecast</a>	All	All	All	All
Application	<a href="#">Xiph</a>	<a href="#">Icecast</a>	All	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] [DLA-1588-1] icecast2 security update	MLIST	<a href="#">lists.debian.org</a>	Thi
oss-security - Icecast 2.4.4 - CVE-2018-18820 - buffer overflow in url-auth	MLIST	<a href="#">www.openwall.com</a>	Ma
Debian -- Security Information -- DSA-4333-1 icecast2	DEBIAN	<a href="#">www.debian.org</a>	Thi
Icecast: Arbitrary code execution (GLSA 201811-09) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	Mit
Icecast url-auth Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">www.securitytracker.com</a>	Thi
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500254](#) Alpine Linux Security Update for icecast

[504004](#) Alpine Linux Security Update for icecast

[710272](#) Gentoo Linux Icecast Arbitrary code execution Vulnerability (GLSA 201811-09)

© [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](#)