



CVE-2020-6095

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

Summary

CVE	CVE-2020-6095
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-27 20:15:00 UTC
Updated	2022-05-12 17:18:00 UTC
Description	An exploitable denial of service vulnerability exists in the GstRTSPAuth functionality of GStreamer/gst-rtsp-server 1.14.5. A

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gstreamer Project	Gst-rtsp-server	1.14.5	All	All	All
Application	Gstreamer Project	Gst-rtsp-server	1.14.5	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference

- [security-announce] openSUSE-SU-2020:0535-1: moderate: Security update f
- TALOS-2020-1018 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- GStreamer RTSP Server: Denial of service (GLSA 202009-05) — Gentoo security
- rtsp-auth: Fix NULL pointer dereference when handling an invalid basic Authorization header (44ccca30) · Commits · GStreamer / gst-rtsp-ser
- 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](#)