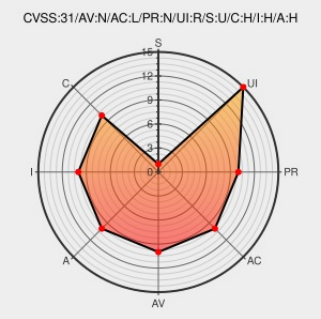
# CVE-2019-15942

Published on: 09/05/2019 12:00:00 AM UTC

Last Modified on: 02/28/2023 02:11:00 PM UTC

## CVE-2019-15942

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Ffmpeg from Ffmpeg contain the following vulnerability:

FFmpeg through 4.2 has a "Conditional jump or move depends on uninitialised value" issue in h2645_parse because alloc_rbsp_buffer in libavcodec/h2645_parse.c mishandles rbsp_buffer.

CVE-2019-15942 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 6.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| #8093 (Uninitialized use in h2645_parse) – FFmpeg | Exploit, Third Party Advisory, trac.ffmpeg.org, text/html | MISC trac.ffmpeg.org/ticket/8093 |

| | | |
|---|---|---|
| [security-announce] openSUSE-SU-2020:0024-1: moderate: Security update f | lists.opensuse.org text/html | SUSE openSUSE-SU-2020:0024 |
| FFmpeg: Multiple vulnerabilities (GLSA 202007-58) — Gentoo security | security.gentoo.org text/html | GENTOO GLSA-202007-58 |



## Related QID Numbers

500908 Alpine Linux Security Update for ffmpeg

502278 Alpine Linux Security Update for ffmpeg4

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Ffmpeg | Ffmpeg | All | All | All | All |

cpe:2.3:a:ffmpeg:ffmpeg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→