



CVE-2018-6360

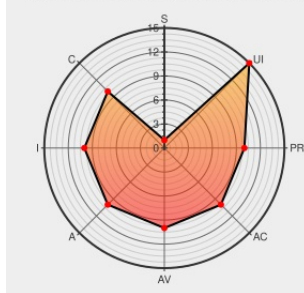
Published on: 01/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6360

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

mpv through 0.28.0 allows remote attackers to execute arbitrary code via a crafted web site, because it reads HTML documents containing VIDEO elements, and accepts arbitrary URLs in a src attribute without a protocol whitelist in player/lua/ytdl_hook.lua. For example, an `av://lavfi:ladspa=file=` URL signifies that the product should call dlopen on a shared object file located at an arbitrary local pathname. The issue exists because the product does not consider that youtube-dl can provide a potentially unsafe URL.

CVE-2018-6360 has been assigned by [M](#) `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
Protocol whitelist in ytdl_hook - Issue #5456	CVE-2018-6360	MISC github.com/mpv-player/mpv/issues/5456

Protocol whitelist in ytdl_hook · Issue #3436 · mpv-player/mpv · GitHub	Exploit Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/mpv-player/mpv/issues/3436
ytdl_hook: whitelist protocols from urls retrieved from youtube-dl · mpv-player/mpv@e6e6b0d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mpv-player/mpv/commit/e6e6b0dcc7e9b0dbf35154a179b3dc1fcfcff43
Debian -- Security Information -- DSA-4105-1 mpv	Third Party Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-4105
mpv: Remote code execution (GLSA 201805-05) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201805-05

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[501080](#) Alpine Linux Security Update for mpv

[710320](#) Gentoo Linux mpv Remote code execution Vulnerability (GLSA 201805-05)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mpv	Mpv	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:mpv:mpv:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)