



# CVE-2018-5002

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-5002
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@adobe.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-09 19:29:00 UTC
<b>Updated</b>	2020-08-24 17:37:00 UTC
<b>Description</b>	Adobe Flash Player versions 29.0.0.171 and earlier have a Stack-based buffer overflow vulnerability. Successful exploitatio

## Risk And Classification

**EPSS:** 0.471450000 probability, percentile 0.977020000 (date 2026-05-05)

**CISA KEV:** Listed on 2022-05-23; due 2022-06-13; ransomware use Unknown

**Problem Types:** CWE-787

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Adobe
<b>Product</b>	Flash Player
<b>Name</b>	Adobe Flash Player Stack-based Buffer Overflow Vulnerability
<b>Required Action</b>	The impacted product is end-of-life and should be disconnected if still in use.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-5002">https://nvd.nist.gov/vuln/detail/CVE-2018-5002</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	All	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	All	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	All	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player Desktop Runtime</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	-	All	All	All
Operating System	<a href="#">Google</a>	<a href="#">Chrome Os</a>	-	All	All	All
Operating System	<a href="#">Google</a>	<a href="#">Chrome Os</a>	-	All	All	All

Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 8.1</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 8.1</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[Adobe Flash Player Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker](#)

[Adobe Flash Player: Multiple vulnerabilities \(GLSA 201806-02\) — Gentoo Security](#)

[Adobe Security Bulletin](#)

[Adobe Flash Player CVE-2018-5002 Stack Buffer Overflow Vulnerability](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[690580](#) Free Berkeley Software Distribution (FreeBSD) Security Update for flash player (2dde5a56-6ab1-11e8-b639-6451062f0f7a)

[710275](#) Gentoo Linux Adobe Flash Player Multiple Vulnerabilities (GLSA 201806-02)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)