



# CVE-2016-7855

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-7855                                                                                                           |
| <b>State</b>           | PUBLISHED                                                                                                               |
| <b>Assigner</b>        | adobe                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2016-11-01 22:59:00 UTC                                                                                                 |
| <b>Updated</b>         | 2026-04-21 21:10:21 UTC                                                                                                 |
| <b>Description</b>     | Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Lin |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.616100000 probability, percentile 0.983490000 (date 2026-05-18)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-416 | n/a | CWE-416 CWE-416 Use After Free

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov                         | Primary   | 8.8   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1     | ADP                                  | DECLARED  | 8.8   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 8.8   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0     | nvd@nist.gov                         | Primary   | 9.3   |          | AV:N/AC:M/Au:N/C:C/I:C/A:C                   |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

|                 |                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------|
| Vendor          | Adobe                                                                                                       |
| Product         | Flash Player                                                                                                |
| Name            | Adobe Flash Player Use-After-Free Vulnerability                                                             |
| Required Action | The impacted product is end-of-life and should be disconnected if still in use.                             |
| Notes           | <a href="https://nvd.nist.gov/vuln/detail/CVE-2016-7855">https://nvd.nist.gov/vuln/detail/CVE-2016-7855</a> |

NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product      | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Application      | Adobe  | Flash Player | All     | All    | All     | All      |
| Application      | Adobe  | Flash Player | All     | All    | All     | All      |
| Application      | Adobe  | Flash Player | All     | All    | All     | All      |
| Application      | Adobe  | Flash Player | All     | All    | All     | All      |
| Operating System | Apple  | Mac Os X     | -       | All    | All     | All      |
| Operating System | Google | Chrome Os    | -       | 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 10</a>          | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 10</a>          | 1511 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows 10</a>          | 1607 | 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 Rt 8.1</a>      | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | r2   | All | All | All |

Vendor Declared Affected Products

| Source | Vendor             | Product             | Version      | Platforms     |
|--------|--------------------|---------------------|--------------|---------------|
| CNA    | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

References

| Reference                                                                                                 | Source                                   |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------|
| Adobe Flash Player CVE-2016-7855 Use After Free Remote Code Execution Vulnerability                       | <a href="#">af854a3a-2127-422b-91ae-</a> |
| Adobe Flash Player: Multiple vulnerabilities (GLSA 201610-10) — Gentoo security                           | <a href="#">af854a3a-2127-422b-91ae-</a> |
| Microsoft Security Bulletin MS16-128 - Critical   Microsoft Docs                                          | <a href="#">af854a3a-2127-422b-91ae-</a> |
| Google Online Security Blog: Disclosing vulnerabilities to protect users                                  | <a href="#">af854a3a-2127-422b-91ae-</a> |
| Red Hat Customer Portal                                                                                   | <a href="#">af854a3a-2127-422b-91ae-</a> |
| <a href="#">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>                                      | <a href="#">134c704f-9b21-4f2e-91b3-</a> |
| Adobe Security Bulletin                                                                                   | <a href="#">af854a3a-2127-422b-91ae-</a> |
| Adobe Flash Player Use-After-Free Memory Error Lets Remote Users Execute Arbitrary Code - SecurityTracker | <a href="#">af854a3a-2127-422b-91ae-</a> |
| CVE Program record                                                                                        | CVE.ORG                                  |
| NVD vulnerability detail                                                                                  | NVD                                      |
| CISA Known Exploited Vulnerabilities catalog                                                              | CISA                                     |

No vendor comments have been submitted for this CVE.

Additional Advisory Data

| Source | Time                     | Event                           |
|--------|--------------------------|---------------------------------|
| ADP    | 2022-03-03T00:00:00.000Z | CVE-2016-7855 added to CISA KEV |

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](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)