



CVE-2015-8049

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

Summary

CVE	CVE-2015-8049
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-10 05:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Air	All	All	All	All

Application	Adobe	Flash Player	19.0.0.185	All	All	All
Application	Adobe	Flash Player	19.0.0.207	All	All	All
Application	Adobe	Flash Player	19.0.0.226	All	All	All
Application	Adobe	Flash Player	19.0.0.245	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference						
[security-announce] SUSE-SU-2015:2236-1: important: Security update for						
[security-announce] openSUSE-SU-2015:2239-1: important: Security update						
ZDI-15-601 Zero Day Initiative						
Adobe Flash Player Multiple Bugs Let Remote Users Bypass Security Controls and Execute Arbitrary Code on the Target System - SecurityTr						
Adobe Flash Player: Multiple vulnerabilities (GLSA 201601-03) — Gentoo Security						
[security-announce] SUSE-SU-2015:2247-1: important: Security update for						
Adobe Flash Player and AIR APSB15-32 Multiple Use After Free Remote Code Execution Vulnerabilities						
Adobe Security Bulletin						
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.