



CVE-2017-3075

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

Summary

CVE	CVE-2017-3075
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-20 17:29:00 UTC
Updated	2018-01-05 02:31:00 UTC
Description	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability when manipulating the A

Risk And Classification

Problem Types: CWE-416

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	Apple	Mac Os X	-	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows 10	All	All	All	All
Operating System	Microsoft	Windows 10	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All

References	
Reference	Source
Adobe Flash Player Use-After-Free and Memory Corruption Errors Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
Adobe Flash Player: Multiple Vulnerabilities (GLSA 201707-15) — Gentoo security	GENTOO
Red Hat Customer Portal	REDHAT
Adobe Security Bulletin	CONFIRM
Adobe Flash Player APSB17-17 Multiple Use After Free Remote Code Execution Vulnerabilities	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
710388 Gentoo Linux Adobe Flash Player Multiple Vulnerabilities (GLSA 201707-15)	