CVE-2017-3063

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-3063
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 14:59:00 UTC
Updated	2018-01-05 02:31:00 UTC
Description	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the ActionScript2 NetS

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
Zero Day Initiative	MISC
Adobe Flash Player APSB17-10 Multiple Use After Free Remote Code Execution Vulnerabilities	BID
Adobe Flash Player: Multiple vulnerabilities (GLSA 201704-04) — Gentoo Security	GENTOO
Red Hat Customer Portal	REDHAT
Adobe Flash Player Use-After-Free and Memory Corruption Errors Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
Adobe Security Bulletin	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710481 Gentoo Linux Adobe Flash Player Multiple Vulnerabilities (GLSA 201704-04)

© 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 registred 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**