CVE-2008-4818

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

Summary

CVE	CVE-2008-4818
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-10 14:12:00 UTC
Updated	2018-10-30 16:26:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Adobe Flash Player 9.0.124.0 and earlier allows remote attackers to inject arbitrar

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	7.0.69.0	All	All	All
Application	Adobe	Flash Player	8.0.39.0	All	All	All
Application	Adobe	Flash Player	9.0	All	All	All
Application	Adobe	Flash Player	9.0.112.0	All	All	All
Application	Adobe	Flash Player	9.0.114.0	All	All	All
Application	Adobe	Flash Player	9.0.115.0	All	All	All
Application	Adobe	Flash Player	9.0.16	All	All	All
Application	Adobe	Flash Player	9.0.16	All	windows	All
Application	Adobe	Flash Player	9.0.18d60	All	All	All
Application	Adobe	Flash Player	9.0.20	All	All	All
Application	Adobe	Flash Player	9.0.20.0	All	All	All
Application	Adobe	Flash Player	9.0.28	All	All	All
Application	Adobe	Flash Player	9.0.28.0	All	All	All
Application	Adobe	Flash Player	9.0.28.0	All	mac_os_x	All
Application	Adobe	Flash Player	9.0.31	All	All	All
Application	Adobe	Flash Player	9.0.31.0	All	All	All
Application	Adobe	Flash Player	9.0.45.0	All	All	All

Application	Adobe	Flash Player	9.0.47.0	All	All	All
Application	Adobe	Flash Player	9.0.48.0	All	All	All
Application	Adobe	Flash Player	7.0.69.0	All	All	All
Application	Adobe	Flash Player	8.0.39.0	All	All	All
Application	Adobe	Flash Player	9.0	All	All	All
Application	Adobe	Flash Player	9.0.112.0	All	All	All
Application	Adobe	Flash Player	9.0.114.0	All	All	All
Application	Adobe	Flash Player	9.0.115.0	All	All	All
Application	Adobe	Flash Player	9.0.16	All	All	All
Application	Adobe	Flash Player	9.0.16	All	windows	All
Application	Adobe	Flash Player	9.0.18d60	All	All	All
Application	Adobe	Flash Player	9.0.20	All	All	All
Application	Adobe	Flash Player	9.0.20.0	All	All	All
Application	Adobe	Flash Player	9.0.28	All	All	All
Application	Adobe	Flash Player	9.0.28.0	All	All	All
Application	Adobe	Flash Player	9.0.28.0	All	mac_os_x	All
Application	Adobe	Flash Player	9.0.31	All	All	All
Application	Adobe	Flash Player	9.0.31.0	All	All	All
Application	Adobe	Flash Player	9.0.45.0	All	All	All
Application	Adobe	Flash Player	9.0.47.0	All	All	All
Application	Adobe	Flash Player	9.0.48.0	All	All	All
Application	Adobe	Flash Player	All	All	All	All

References

Reference	Sou
Gentoo update for netscape-flash - Secunia Advisories - Vulnerability Information - Secunia.com	SEC
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
Adobe Flash Player Multiple Security Vulnerabilities	BID
ASA-2009-020 (SUN 248586)	CON
Nortel: Technical Support: Nortel Response to Sun Alert 248586 - Multiple Security Vulnerabilities in the Flash Player Plugin for Solaris	CON
Adobe Flash Player HTTP Response Header Processing Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SEC
Adobe - Security Advisories: APSB08-20 - Flash Player update available to address security vulnerabilities	CON
About Secunia Research | Flexera	SEC
IBM X-Force Exchange	XF
ASA-2008-440 (RHSA-2008-0980)	CON

Support	REL
Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities	GEN
Red Hat update for flash-plugin - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
248586	SUN
APPLE-SA-2008-12-15 Security Update 2008-008 / Mac OS X v10.5.6	APF
US-CERT Technical Cyber Security Alert TA08-350A -- Apple Updates for Multiple Vulnerabilities	CEF
About the security content of Security Update 2008-008 / Mac OS X v10.5.6	CON
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**