CVE-2018-4878

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-4878
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-06 21:29:00 UTC
Updated	2022-04-18 14:26:00 UTC
Description	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a da

Risk And Classification

EPSS: 0.933610000 probability, percentile 0.998090000 (date 2026-04-02)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Known

Problem Types: CWE-416

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	https://nvd.nist.gov/vuln/detail/CVE-2018-4878

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
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	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	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
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference
Flash Exploit, CVE-2018-4878, Spotted in The Wild as Part of Massive Malspam Campaign
North Korean Hackers Allegedly Exploit Adobe Flash Player Vulnerability (CVE-2018-4878) Against South Korean Targets - Security News - T
Adobe Flash Player Use-After-Free Memory Error Lets Remote Users Execute Arbitrary Code - SecurityTracker
Adobe Flash < 28.0.0.161 - Use-After-Free - Multiple remote Exploit
Talos Blog || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Flash 0-Day In The Wild: Group 123 At The Controls
Adobe Flash Player Zero-Day Spotted in the Wild | The first stop for security news | Threatpost
Adobe Flash Vulnerability Reappears in Malicious ...
malware-samples/CVE-2018-4878-Adobe-Flash-DRM-UAF-0day at master · InQuest/malware-samples · GitHub
How Hackers Bypassed an Adobe Flash Protection Mechanism | McAfee Blogs
GitHub - vysec/CVE-2018-4878: Aggressor Script to launch IE driveby for CVE-2018-4878
Adobe Security Bulletin
Attacks Leveraging Adobe Zero-Day (CVE-2018-4878) – Threat Attribution, Attack Scenario and Recommendations « Attacks Leveraging Adc
Adobe Flash Player CVE-2018-4878 Use After Free Remote Code Execution Vulnerability

Red Hat Customer Portal
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

690574 Free Berkeley Software Distribution (FreeBSD) Security Update for flash player (756a8631-0b84-11e8-a986-6451062f0f7a)

710234 Gentoo Linux Adobe Flash Player Multiple Vulnerabilities (GLSA 201803-08)