



## EXECUTIVE SUMMARY

September 11, 2019 | MTIS19-044

Since the last McAfee® Labs Security Advisory (September 10), the following noteworthy event has taken place:

- Patches are available for multiple Adobe security vulnerabilities.

## NEW THREAT OVERVIEW

### (APSB19-46) Adobe Flash Same Origin Method Execution Remote Code Execution (CVE-2019-8069)

MTIS19-044-A

IMPORTANCE: **Medium**  
 COVERED PRODUCTS:  
 UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

[Back to top](#)

### (APSB19-46) Adobe Flash Use After Free Remote Code Execution (CVE-2019-8070)

MTIS19-044-B

IMPORTANCE: **Medium**  
 COVERED PRODUCTS:  
 UNDER ANALYSIS: DAT | Web Gateway | Firewall Enterprise

[Back to top](#)

## THREAT DETAILS

### (APSB19-46) Adobe Flash Same Origin Method Execution Remote Code Execution (CVE-2019-8069)

MTIS19-044-A

|                                     |  |
|-------------------------------------|--|
| <b>THREAT IDENTIFIER(S)</b>         | CVE-2019-8069  |
| <b>THREAT TYPE</b>                  | Vulnerability  |
| <b>RISK ASSESSMENT</b>              | Medium   |
| <b>MAIN THREAT VECTORS</b>          | Locally logged-on user   |
| <b>USER INTERACTION REQUIRED</b>    | Yes  |
| <b>DESCRIPTION</b>                  | A vulnerability in some versions of Adobe Flash could lead to remote code execution. The flaw lies in the Same Origin Method Execution component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document. |
| <b>IMPORTANCE</b>                   | Medium. On September 10, Adobe released an update to address this vulnerability  |
| <b>MCAFFEE PRODUCT COVERAGE</b>     |  |
| DAT FILES                           | Under analysis   |
| VIRUS SCAN ENTERPRISE SCAN BOP      | Out of scope   |
| HOST IPS                            | Out of scope   |
| NETWORK SECURITY PLATFORM           | Coverage not warranted   |
| VULNERABILITY MANAGER               | An upcoming FSL/MVM content release will contain coverage for this issue.  |
| WEB GATEWAY                         | Under analysis   |
| REMEDIATION MANAGER                 | Not applicable   |
| POLICY AUDITOR                      | An upcoming SCAP content release will contain coverage for this issue.   |
| NETWORK ACCESS CONTROL              | An upcoming SCAP content release will contain coverage for this issue.   |
| FIREWALL ENTERPRISE                 | Under analysis   |
| APPLICATION CONTROL                 | Out of scope   |
| DATABASE ACTIVITY MONITORING        | Out of scope   |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope   |
| <b>ADDITIONAL INFORMATION</b>       | <a href="#">Adobe: Security Bulletins and Advisories</a>   |

[Back to top](#)

**(APSB19-46) Adobe Flash Use After Free Remote Code Execution (CVE-2019-8070)**

MTIS19-044-B

|                                     |  |
|-------------------------------------|--|
| <b>THREAT IDENTIFIER(S)</b>         | CVE-2019-8070  |
| <b>THREAT TYPE</b>                  | Vulnerability  |
| <b>RISK ASSESSMENT</b>              | Medium   |
| <b>MAIN THREAT VECTORS</b>          | Web  |
| <b>USER INTERACTION REQUIRED</b>    | Yes  |
| <b>DESCRIPTION</b>                  | A vulnerability in some versions of Adobe Flash could lead to remote code execution. The flaw lies in the Use After Free component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document. |
| <b>IMPORTANCE</b>                   | Medium. On September 10, Adobe released an update to address this vulnerability  |
| <b>MCAFFEE PRODUCT COVERAGE</b>     |  |
| DAT FILES                           | Under analysis   |
| VIRUS SCAN ENTERPRISE SCAN BOP      | Out of scope   |
| HOST IPS                            | Out of scope   |
| NETWORK SECURITY PLATFORM           | Coverage not warranted   |
| VULNERABILITY MANAGER               | An upcoming FSL/MVM content release will contain coverage for this issue.  |
| WEB GATEWAY                         | Under analysis   |
| REMIEDIATION MANAGER                | Not applicable   |
| POLICY AUDITOR                      | An upcoming SCAP content release will contain coverage for this issue.   |
| NETWORK ACCESS CONTROL              | An upcoming SCAP content release will contain coverage for this issue.   |
| FIREWALL ENTERPRISE                 | Under analysis   |
| APPLICATION CONTROL                 | Out of scope   |
| DATABASE ACTIVITY MONITORING        | Out of scope   |
| VULNERABILITY MANAGER FOR DATABASES | Out of scope   |
| <b>ADDITIONAL INFORMATION</b>       | <a href="#">Adobe: Security Bulletins and Advisories</a>   |

[Back to top](#)

---

For McAfee Technical Support, [click here](#).

For Multi-National Phone Support, [click here](#).

McAfee values your feedback on this Security Advisory. Please reply to this mail with your comments.

\*The information provided is only for the use and convenience of McAfee's customers in connection with their McAfee products, and applies only to the threats described herein. McAfee product coverage statements are limited to known attack vectors and should not be considered comprehensive. THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS IS" AND IS SUBJECT TO CHANGE WITHOUT NOTICE.

The information contained herein is the property of McAfee, LLC and may not be reproduced or disseminated without the expressed written consent of McAfee, LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

McAfee, Inc. 2821 Mission College Blvd, Santa Clara, CA 95054 888.847.8766 [www.mcafee.com](http://www.mcafee.com)

© 2018 McAfee, LLC. All rights reserved.