Solution Brief

Protecting Against Adobe Flash Exploits

The multimedia and software platform Adobe Flash is a very popular way to deliver rich web-based content such as games, websites, applications, and more. Unfortunately, its popularity makes it an attractive target for cybercriminals, who ruthlessly exploit new, unpatched vulnerabilities to compromise unsuspecting users.

Prevalence of Adobe Flash exploitation

Flash exploits are discussed in depth in the ***McAfee Labs Threats Report: May 2015***. Flash exploits began to increase dramatically beginning in the last quarter of 2014. Flash vulnerabilities are now among the main targets of exploit authors. McAfee Labs believes this is due to the steady increase in the number of Flash vulnerabilities; user delay in the application of software patches for those vulnerabilities; new, creative methods to exploit them; a steep increase in the number of mobile devices that can play Flash .swf files; and the difficulty of detecting Flash exploits.

Among the exploit kits delivering Flash exploits, Angler has become the most popular. This powerful kit, discussed in depth in the ***McAfee Labs Threat Report: February 2015***, is an off-the-shelf, easy-to-use toolkit that can deliver a wide variety of payloads through the exploitation of vulnerabilities.

Safeguarding against Flash exploits

Here are some good practices and procedures to protect against Flash exploits:

- Enable automatic operating system updates, or download operating system updates regularly, to keep them patched against known vulnerabilities.
- Configure antivirus software to block attachments containing the .swf extension.
- Configure the browser security settings to medium level or above.
- Use a browser plug-in to block the execution of scripts and iframes.
- Do not install untrusted browser plug-ins.
- Use great caution when opening attachments, especially when those attachments carry the .swf extension.
- Never open unsolicited emails, or unexpected attachments—even from known people.
- Beware of spam-based phishing schemes. Do not click on links in emails or instant messages.
- Type the URLs or copy the URLs to the address bar of the browser and verify the address rather than clicking on web advertisements.
- Do not click on Flash movies on untrusted websites.

How Intel Security can help protect against Flash exploits

McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in trusted websites are just some of the attack methods used to deliver attacks that leverage Flash exploits. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway anti-malware engine:** Signatureless intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protect against zero-day and targeted attacks. The gateway anti-malware engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee Global Threat Intelligence (McAfee GTI):** Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

McAfee Application Control

McAfee Application Control lets your company control which applications are allowed to run in your environment through dynamic whitelisting and enforcement policies on both connected and disconnected endpoints. Ensuring your organization is protected against vulnerable applications such as outdated Flash installations is key to combating the growing trend of Flash exploits.

- **Dynamic whitelisting:** Enable your organization to efficiently manage your whitelisted applications by developing the whitelist automatically as systems are patched and updated. McAfee Application Control reduces your exposure to Flash exploits by ensuring unpatched versions of Flash are not allowed to run in your environment.
- **File reputation:** Integration with McAfee GTI allows McAfee Application Control to query real-time feeds of known good, bad, and unknown file types to help your company stay aware of vulnerabilities or attacks from applications that may have been altered.
- **Protection whether connected or disconnected:** Enforce controls on connected or disconnected servers, virtual machines, endpoints, and fixed-function devices such as point-of-sale terminals.

McAfee Vulnerability Manager

McAfee Vulnerability Manager helps your organization understand the scope of exposure that can result from having old versions of Flash in your environment and take the necessary steps to effectively reduce that exposure.

- **Comprehensive vulnerability scanning:** McAfee Vulnerability Manager is a highly scalable standalone product for host discovery, asset management, vulnerability assessment, and reporting on any network-connected device. McAfee Vulnerability Manager can assess your environment's exposure to Flash exploits by scanning for systems running vulnerable versions of Flash.
- **Flexible reporting and remediation:** McAfee Vulnerability Manager and **McAfee Asset Manager** work together to provide automated monitoring and management of scanning, remediation, enforcement, and reporting. This helps you avoid time-consuming fire drills and ad hoc processes, eliminate errors, and efficiently protect more systems.
- **Know your exposure:** McAfee Asset Manager lets your company know which systems are vulnerable to Flash exploits by correlating vulnerability scans with host discovery scans. Identifying in realtime which systems are running vulnerable Flash versions means less time wondering if you are exposed and more time on remediation.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt to suit your environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks thanks to its visibility into immediate threats such as unknown files or applications that exploit Flash vulnerabilities in your organization's environment.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation:** McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from running in the environment. If an application that was allowed to execute is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process' actions from installation to the present enables faster response and remediation.
- **Indicators of compromise (IoCs):** Import known bad files hashes and McAfee Threat Intelligence Exchange can immunize your environment against these known bad files through policy enforcement. If any of the IoCs trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the IoC.

McAfee VirusScan Enterprise

Detecting and cleaning malware that exploits Flash vulnerabilities to infiltrate your environment is simple with **McAfee VirusScan® Enterprise**. McAfee VirusScan Enterprise uses the award-winning McAfee scanning engine to protect your files from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks:** Integrates anti-malware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in applications.
- **Unbeatable malware detection and cleaning:** Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques that include port blocking, filename blocking, folder/directory lockdown, file-share lockdown, and infection tracing and blocking.
- **Real-time security with McAfee GTI integration:** Protects against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in market.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) is a comprehensive, real-time, cloud-based threat intelligence service that enables McAfee products to block cyber threats across all vectors—file, web, message, and network. Proactively protect against Flash exploits and others with these features:

- **Intelligence through vector correlation:** Collects and correlates data from and across all key threat vectors—file, web, email, and network—to detect blended threats.
- **Comprehensive threat intelligence platform:** Collects threat intelligence from millions of sensors on customer-deployed McAfee products such as endpoint, web, mail, network intrusion prevention systems, and firewall devices.
- **Security Connected:** Integrates with other McAfee security products to provide the broadest threat data, deepest data correlation, and most complete product integration available today to ensure protection against Flash exploits.

McAfee VirusScan Mobile

McAfee VirusScan Mobile is an anti-malware system that scans and cleans mobile data, preventing corruption from viruses, Trojans, and other malicious code. McAfee VirusScan Mobile protects your mobile devices at the most critical points of exposure, including inbound and outbound emails, text messages, email attachments, and Internet downloads.

- Detect threats in realtime: Block malware in email, text messages, and attachments without any noticeable delay. McAfee VirusScan Mobile scans for a range of malicious threats in fewer than 200 milliseconds, providing automatic and comprehensive protection for smartphones.

The growing prevalence of Flash vulnerabilities being leveraged by malware authors does not show any sign of easing. Intel Security technology can help your company proactively protect itself against threats that seek to exploit those vulnerabilities.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com